SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL ITEMS
OFFEROR TO COMPLETE BLOCKS 12, 17, 23, 24, & 30

1. REQUISITION NUMBER: E009701048A

PAGE 1 OF 35

2. CONTRACT NO.: BBGCON1808C6700

3. AWARD/ EFFECTIVE DATE:

4. ORDER NUMBER:

5. SOLICITATION NUMBER: BBGCON1808S6700

6. SOLICITATION ISSUE DATE: 04/02/0

7. FOR SOLICITATION INFORMATION CALL:
a. NAME: Berel Dorfman
b. TELEPHONE NUMBER (*No collect calls*): (b)(6)

8. OFFER DUE DATE/LOCAL TIME:

9. ISSUED BY — CODE: M/CON/CR

Broadcasting Board of Governors
International Broadcasting Bureau
Office of Contracts (M/CON)
Room 4700, Switzer Building
330 C Street (SW)
Washington DC 20237

10. THIS ACQUISITION IS ☒ UNRESTRICTED OR □ SET ASIDE: % FOR:
□ SMALL BUSINESS □ EMERGING SMALL BUSINESS
□ HUBZONE SMALL BUSINESS
□ SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS □ 8(A)
NAICS:
SIZE STANDARD:

11. DELIVERY FOR FOB DESTINATION UNLESS BLOCK IS MARKED
□ SEE SCHEDULE

12. DISCOUNT TERMS: Net 30

□ 13a. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700)

13b. RATING:

14. METHOD OF SOLICITATION: □ RFQ □ IFB □ RFP

15. DELIVER TO — CODE: E/TT-KD

Kelly DeYoe
Broadcasting Board of Governors
International Broadcasting Bureau
330 C Street, SW, Room 4239
Washington DC 20237

16. ADMINISTERED BY — CODE: M/CON/CR

Broadcasting Board of Governors
International Broadcasting Bureau
Office of Contracts (M/CON)
Room 4700, Switzer Building
330 C Street (SW)
Washington DC 20237

17a. CONTRACTOR/ OFFEROR — CODE: 809211100 — FACILITY CODE:

THE TOR PROJECT, INC.
Attn: Andrew Lewman
122 Scott Circle
Dedham MA 02026

TELEPHONE NO.: (b) (6)

□ 17b. CHECK IF REMITTANCE IS DIFFERENT AND PUT SUCH ADDRESS IN OFFER

18a. PAYMENT WILL BE MADE BY — CODE: CFO/A

Broadcasting Board of Governors
International Broadcasting Bureau
Office of Financial Operations
CFO/A, Room 1655
330 Independence Ave., S.W.
Washington, DC 20237

18b. SUBMIT INVOICES TO ADDRESS SHOWN IN BLOCK 18a UNLESS BLOCK BELOW IS CHECKED □ SEE ADDENDUM

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
	Tax ID Number: 20-8096820 DUNS Number: 809211100 Contractor shall provide enhancements to TOR software system to meet the requirements cited in the Agency's Statement of Work (SOW) attached hereto (Addendum A). Period of Performance: 04/18/2008 to 04/17/2009				
0001	C.2.1 Continued design and development of enhancements to the existing TOR Software, C.2.2 Continued ...				70,000.00

(Use Reverse and/or Attach Additional Sheets as Necessary)

25. ACCOUNTING AND APPROPRIATION DATA: 9568-08-0206-E009701048A

26. TOTAL AWARD AMOUNT (*For Govt. Use Only*): $360,000.00

□ 27a. SOLICITATION INCORPORATES BY REFERENCE FAR 52.212-1, 52.212-4. FAR 52.212-3 AND 52.212-5 ARE ATTACHED. ADDEND □ ARE □ ARE NOT ATTACHED

☒ 27b. CONTRACT/PURCHASE ORDER INCORPORATES BY REFERENCE FAR 52.212-4. FAR 52.212-5 IS ATTACHED. ADDENDA ☒ ARE □ ARE NOT ATTACHED

☒ 28. CONTRACTOR IS REQUIRED TO SIGN THIS DOCUMENT AND RETURN 1 COPIES TO ISSUING OFFICE. CONTRACTOR AGREES TO FURNISH AND DELIVER ALL ITEMS SET FORTH OR OTHERWISE IDENTIFIED ABOVE AND ON ANY ADDITIONAL SHEETS SUBJECT TO THE TERMS AND CONDITIONS SPECIFIED HEREIN.

□ 29. AWARD OF CONTRACT REF. ______ OFFER DATED ______. YOUR OFFER ON SOLICITATION (BLOCK 5), INCLUDING ANY ADDITIONS OR CHANGES WHICH ARE SET FORTH HEREIN, IS ACCEPTED AS TO ITEMS:

30a. SIGNATURE OF OFFEROR/CONTRACTOR:

31a. UNITED STATES OF AMERICA (*SIGNATURE OF CONTRACTING OFFICER*):

30b. NAME AND TITLE OF SIGNER (*Type or print*):

30c. DATE SIGNED:

31b. NAME OF CONTRACTING OFFICER (*Type or print*): Herman Shaw

31c. DATE SIGNED:

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
	Contrator shall submit system architecture and technical design documentation for TOR enhancemnets for review by AR/CO. Obligated Amount: $70,000.00				
0002	C.2.3 Continue development and implementation of the bridge relay mechanism, C.2.4 Contniue development and implementation of the brigde directory authority mechanism, C.2.12 Continued development and implementation to the bridge relay and bridge directory mechanism. Obligated Amount: $80,000.00				80,000.00
0003	C.2.5 Continue design and develop revisions to the TOR network protocols to hide network signature of TOR traffic. Obligated Amount: $20,000.00				20,000.00
0004	C.2.6 Continue to develop and implement enhancements to TOR's cell-based protocol, C.2.7 Continue development of TOR network scalability, and C.2.13 Research and document additional options for the scalability of the TOR network beyond 2 million concurrent users. Obligated Amount: $80,000.00				80,000.00
	Continued ...				

32a. QUANTITY IN COLUMN 21 HAS BEEN

□ RECEIVED □ INSPECTED □ ACCEPTED, AND CONFORMS TO THE CONTRACT, EXCEPT AS NOTED:

32b. SIGNATURE OF AUTHORIZED GOVERNMENT REPRESENTATIVE

32c. DATE

32d. PRINTED NAME AND TITLE OF AUTHORIZED GOVERNMENT REPRESENTATIVE

32e. MAILING ADDRESS OF AUTHORIZED GOVERNMENT REPRESENTATIVE

32f. TELEPHONE NUMBER OF AUTHORIZED GOVERNMENT REPRESENTATIVE

32g. E-MAIL OF AUTHORIZED GOVERNMENT REPRESENTATIVE

33. SHIP NUMBER

□ PARTIAL □ FINAL

34. VOUCHER NUMBER

35. AMOUNT VERIFIED CORRECT FOR

36. PAYMENT

□ COMPLETE □ PARTIAL □ FINAL

37. CHECK NUMBER

38. S/R ACCOUNT NUMBER

39. S/R VOUCHER NUMBER

40. PAID BY

41a. I CERTIFY THIS ACCOUNT IS CORRECT AND PROPER FOR PAYMENT

41b. SIGNATURE AND TITLE OF CERTIFYING OFFICER

41c. DATE

42a. RECEIVED BY *(Print)*

42b. RECEIVED AT *(Location)*

42c. DATE REC'D *(YY/MM/DD)*

42d. TOTAL CONTAINERS

CONTINUATION SHEET	REFERENCE NO. OF DOCUMENT BEING CONTINUED BBGCON1808C6700	PAGE 3	OF 35

NAME OF OFFEROR OR CONTRACTOR
THE TOR PROECT, INC.

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
0005	C.2.8 Continue to work with IBB staff and other IBB contractors to identify tasks in support of this program, and C.2.9 Communicate tasks identified in C.2.8 to the AR/CO and negotitae time frames for their completion. Obligated Amount: $0.00				0.00
0006	C.2.10 Promote active growth of the TOR server network and advocy of TOR products. Obligated Amount: $20,000.00				20,000.00
0007	C.2.11 Improve the ease of use of TOR for end users by continuing research and development. Obligated Amount: $20,000.00				20,000.00
0008	C.2.14 Continue reaserch into the option of providing incentives for TOR users to run TOR relay servers. Obligated Amount: $30,000.00				30,000.00
0009	C.2.15 Develop a more relaible download mechanism for teh TOR browser bundle for users on slow and/or unrelaible network connections. Obligated Amount: $10,000.00				10,000.00
0010	C.2.16 Test the TOR bundle browser in multiple computer systems and analyze these systems for any changes to the system that may have bene made inadvertently by use of the TOR browser bundle. Obligated Amount: $10,000.00				10,000.00
0011	C.2.17 Develop or adapt existing open source software to implement a web-based portal to manage the translation of text into multiple languages for the user interface text or software or Torbutton and Vadalia and other software that may be included in the TOR web browser. Obligated Amount: $20,000.00 Continued ...				20,000.00

CONTINUATION SHEET	REFERENCE NO. OF DOCUMENT BEING CONTINUED BBGCON1808C6700	PAGE 4	OF 35

NAME OF OFFEROR OR CONTRACTOR

THE TOR PROECT, INC.

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	The total amount of award: $360,000.00. The obligation for this award is shown in box 26.				

Addendum "A" – STATEMENT OF WORK

SECTION C

C.1 BACKGROUND

The Broadcasting Board of Governors (BBG) oversees the mission and operation of several overseas broadcasting entities of the United States Government (USG). The International Broadcasting Bureau (IBB) oversees the daily operations of several USG broadcasters, including the Voice of America (VOA), and is responsible for all contractual and fiscal matters pertaining to broadcast operations. The IBB's Internet anti-censorship program seeks to ensure Internet users in target countries are able to access USG broadcasters' web sites to access their news and other programming, using a variety of tools to counter foreign government-sponsored Internet censorship controls.

This Statement of Work defines those duties the Contractor shall perform to enable the IBB to meet its goals of using Tor as a tool to further its Internet anti-censorship efforts.

C.2 TECHNICAL REQUIREMENTS

C.2.1 The Contractor shall continue design and development of enhancements to the existing Tor software to increase its suitability as a tool for Internet users in countries with government-sponsored Internet censorship to circumvent censorship controls, based on the existing research and documentation performed during the previous contract period (e.g. as described in the paper "Design of a blocking-resistant anonymity system").

C.2.2 The Contractor shall submit system architecture and technical design documentation for Tor enhancements specifically related to anti-censorship improvements in C.2.1 to the Authorized Representative of the Contracting Officer (AR/CO) for review and approval before implementation. Significant changes to the design that are discovered during implementation must be documented and reviewed by the AR/CO as soon as the Contractor becomes aware of the need for these revisions.

C.2.3 The Contractor shall continue to develop and implement the bridge relay mechanism as designed during the previous contract period to allow individual Tor users to easily reconfigure their Tor client to automatically relay traffic from users in countries with government-imposed Internet censorship so as to circumvent that censorship.

C.2.4 The Contractor shall continue to develop and implement the bridge directory authority mechanism as designed during the previous contract period to allow Tor clients configured as bridge relays (as described in C.2.3) to communicate their existence to the bridge directory authority, and to allow users in countries with government-imposed Internet censorship to discover addresses of available bridge relays so that they may access the Tor network.

C.2.5 The Contractor shall design and develop revisions to the Tor network protocols to hide the network signature of Tor traffic so it is difficult for government-sponsored Internet censors to identify Tor traffic and trivially block it.

C.2.6 The Contractor shall continue to develop and implement enhancements to Tor's cell-based protocol to improve performance on substandard network connections including those with low bandwidth and/or high latency and/or high packet loss.

C.2.7 The Contractor shall continue development of Tor network scalability, with the goal of supporting 2 million or more concurrent end users. This requirement is only a goal for system scalability and is not a requirement on number of actual concurrent users of the Tor network.

C.2.8 The Contractor shall work with IBB staff and other IBB contractors to identify tasks in support of this program that might be developed collaboratively with Contractor. Tasks involving areas such as documentation, bug fixes, software testing, and any area where specific knowledge of foreign government-sponsored Internet censorship may be especially appropriate for this purpose.

C.2.9 The Contractor shall communicate tasks identified for delegation to IBB in C.2.8 to the AR/CO and negotiate time frames for their completion. The Contractor shall monitor and coordinate work performed by IBB staff on delegated tasks and integrate it into Tor software releases as appropriate.

C.2.10 The Contractor shall promote active growth of the Tor server network and advocacy of Tor products to increase the performance, stability, and usability of Tor, with a focus on the end user experience for users in countries with government-sponsored Internet censorship.

C.2.11 The Contractor shall improve the ease of use of Tor for end users by continuing research and development of one or both of the following products: (1) all-in-one software bundle containing Tor and supporting applications, as well as an easy-to-use installer for Microsoft Windows operating systems, as well as option to install and run from a Universal Serial Bus (USB) flash device; (2) bootable CD-ROM image ("LiveCD") which contains a minimal operating system, Tor, and supporting applications. Both would have all appropriate applications pre-configured to use Tor out of the box with only minimal additional configuration required by the end user. If Contractor determines it is not feasible to develop both products, Contractor will provide detailed written technical analysis and explanation to the AR/CO. The Contractor shall make an initial public release of at least one of these products during the term of this contract.

C.2.12 The Contractor shall continue to develop and implement improvements to the bridge relay and bridge directory authority mechanisms to improve the usability, performance and reliability of the Tor network by users in countries with government-imposed Internet censorship.

C.2.13 The Contractor shall research and document additional options for the scalability of the Tor network beyond 2 million concurrent users, including analysis of splitting the network into multiple segments, switching to datagram-based protocols, and improving the load balancing within the network.

C.2.14 The Contractor shall continue research into the option of providing incentives for Tor users to run Tor relay servers. If further research indicates that this should be pursued, the Contractor shall develop a project plan and timeline for this work. If further research indicates this option should be abandoned, the Contractor shall document and explain in writing the reasoning behind this decision.

C.2.15 The Contractor shall develop a more reliable download mechanism for the Tor browser bundle for users on slow and/or unreliable network connections, by means of a split download of multiple smaller files, implementation of a lightweight download manager, reduction in the software bundle file size, or other method as chosen by the Contractor.

C.2.16 The Contractor shall test the Tor browser bundle on multiple computer systems and analyze these systems afterwards for any changes to the system that may have been made inadvertently by use of the Tor browser bundle. The Contractor shall document any such changes found and develop a plan to reduce the footprint of Tor browser bundle use.

C.2.17 The Contractor shall develop or adapt existing open source software to implement a web-based portal to manage the translations of text into multiple languages for the user interface text of software of Torbutton and Vidalia and other software that may in the future be included in the Tor browser bundle. The web site must allow non-technical users the ability to contribute translations by providing text to be translated in English, as well as any needed context on the use of the text, and allowing users to enter the translation into their language from their web browser.

C.3 <u>ADMINISTRATIVE REQUIREMENTS</u>

C.3.1 The Contractor shall provide a Monthly Status Report within ten (10) business days of the end of the month to the AR/CO detailing work performed during the previous month. This report shall describe the work performed for specific requirements of this contract. The report shall also include any other relevant information on Tor activities that may have indirect impacts on contracted work.

C.3.2 The Contractor shall be available for a telephone conference call with the AR/CO, other IBB staff and representatives at a mutually agreeable time on a periodic basis averaging no more than 2 calls per month of one hour's duration. This requirement is in addition to any other required communication by telephone or email with the AR/CO for execution of this contract.

C.4 ADDITIONAL TERMS

C.4.1 All software and accompanying documentation developed under the terms of this contract must be distributed under an open source software license, such as the "BSD License" or other commonly accepted open source software license as mutually agreed upon by the Contractor and the AR/CO.

Addendum "B" – PRICING SCHEDULE

Item Number	Description	Fixed Price
C.2.1 & C.2.2	See SOW C.2.1 & C.2.2	___________
C.2.3, C.2.4, & C.2.12	See SOW C.2.3, C.2.4, & C.2.12	___________
C.2.5	See SOW C.2.5	___________
C.2.6, C.2.7, & C.2.13	See SOW C.2.6, C.2.7, & C.2.13	___________
C.2.8 & C.2.9	See SOW C.2.8 & C.2.9	___________
C.2.10	See SOW C.2.10	___________
C.2.11	See SOW C.2.11	___________
C.2.14	See SOW C.2.14	___________
C.2.15	See SOW C.2.15	___________
C.2.16	See SOW C.2.16	___________
C.2.17	See SOW C.2.17	___________

Total Firm Fixed Price contract $___________

52.212-4 -- Contract Terms and Conditions -- Commercial Items.

As prescribed in 12.301(b)(3), insert the following clause:

Contract Terms and Conditions -- Commercial Items (Feb 2007)

(a) *Inspection/Acceptance.* The Contractor shall only tender for acceptance those items that conform to the requirements of this contract. The Government reserves the right to inspect or test any supplies or services that have been tendered for acceptance. The Government may require repair or replacement of nonconforming supplies or reperformance of nonconforming services at no increase in contract price. If repair/replacement or reperformance will not correct the defects or is not possible, the government may seek an equitable price reduction or adequate consideration for acceptance of nonconforming supplies or services. The Government must exercise its post-acceptance rights --

(1) Within a reasonable time after the defect was discovered or should have been discovered; and

(2) Before any substantial change occurs in the condition of the item, unless the change is due to the defect in the item.

(b) *Assignment.* The Contractor or its assignee may assign its rights to receive payment due as a result of performance of this contract to a bank, trust company, or other financing institution, including any Federal lending agency in accordance with the Assignment of Claims Act (31 U.S.C.3727). However, when a third party makes payment (*e.g.,* use of the Governmentwide commercial purchase card), the Contractor may not assign its rights to receive payment under this contract.

(c) *Changes.* Changes in the terms and conditions of this contract may be made only by written agreement of the parties.

(d) *Disputes.* This contract is subject to the Contract Disputes Act of 1978, as amended (41 U.S.C. 601-613). Failure of the parties to this contract to reach agreement on any request for equitable adjustment, claim, appeal or action arising under or relating to this contract shall be a dispute to be resolved in accordance with the clause at FAR 52.233-1, Disputes, which is incorporated herein by reference. The Contractor shall proceed diligently with performance of this contract, pending final resolution of any dispute arising under the contract.

(e) *Definitions.* The clause at FAR 52.202-1, Definitions, is incorporated herein by reference.

(f) *Excusable delays.* The Contractor shall be liable for default unless nonperformance is caused by an occurrence beyond the reasonable control of the Contractor and without its fault or negligence such as, acts of God or the public enemy, acts of the Government in either its sovereign or contractual capacity, fires, floods, epidemics, quarantine restrictions, strikes, unusually severe weather, and delays of common carriers. The Contractor shall notify the Contracting Officer in writing as soon as it is reasonably possible after the commencement of any excusable delay, setting forth the full particulars in connection therewith, shall remedy such occurrence with all reasonable dispatch, and shall promptly give written notice to the Contracting Officer of the cessation of such occurrence.

(g) *Invoice.*

(1) The Contractor shall submit an original invoice and three copies (or electronic invoice, if authorized) to the address designated in the contract to receive invoices. An invoice must include --

(i) Name and address of the Contractor;

(ii) Invoice date and number;

(iii) Contract number, contract line item number and, if applicable, the order number;

(iv) Description, quantity, unit of measure, unit price and extended price of the items delivered;
(v) Shipping number and date of shipment, including the bill of lading number and weight of shipment if shipped on Government bill of lading;
(vi) Terms of any discount for prompt payment offered;
(vii) Name and address of official to whom payment is to be sent;
(viii) Name, title, and phone number of person to notify in event of defective invoice; and
(ix) Taxpayer Identification Number (TIN). The Contractor shall include its TIN on the invoice only if required elsewhere in this contract.
(x) Electronic funds transfer (EFT) banking information.
(A) The Contractor shall include EFT banking information on the invoice only if required elsewhere in this contract.
(B) If EFT banking information is not required to be on the invoice, in order for the invoice to be a proper invoice, the Contractor shall have submitted correct EFT banking information in accordance with the applicable solicitation provision, contract clause (*e.g.*, 52.232-33, Payment by Electronic Funds Transfer—Central Contractor Registration, or 52.232-34, Payment by Electronic Funds Transfer—Other Than Central Contractor Registration), or applicable agency procedures.
(C) EFT banking information is not required if the Government waived the requirement to pay by EFT.
(2) Invoices will be handled in accordance with the Prompt Payment Act (31 U.S.C. 3903) and Office of Management and Budget (OMB) prompt payment regulations at 5 CFR part 1315.

(h) *Patent indemnity*. The Contractor shall indemnify the Government and its officers, employees and agents against liability, including costs, for actual or alleged direct or contributory infringement of, or inducement to infringe, any United States or foreign patent, trademark or copyright, arising out of the performance of this contract, provided the Contractor is reasonably notified of such claims and proceedings.

(i) *Payment*.

(1) Items accepted. Payment shall be made for items accepted by the Government that have been delivered to the delivery destinations set forth in this contract.
(2) Prompt Payment. The Government will make payment in accordance with the Prompt Payment Act (31 U.S.C. 3903) and prompt payment regulations at 5 CFR Part 1315.
(3) Electronic Funds Transfer (EFT). If the Government makes payment by EFT, see 52.212-5(b) for the appropriate EFT clause.
(4) Discount. In connection with any discount offered for early payment, time shall be computed from the date of the invoice. For the purpose of computing the discount earned, payment shall be considered to have been made on the date which appears on the payment check or the specified payment date if an electronic funds transfer payment is made.
(5) Overpayments. If the Contractor becomes aware of a duplicate contract financing or invoice payment or that the Government has otherwise overpaid on a contract financing or invoice payment, the Contractor shall immediately notify the Contracting Officer and request instructions for disposition of the overpayment.

(j) *Risk of loss*. Unless the contract specifically provides otherwise, risk of loss or damage to the supplies provided under this contract shall remain with the Contractor until, and shall pass to the Government upon:

(1) Delivery of the supplies to a carrier, if transportation is f.o.b. origin; or

(2) Delivery of the supplies to the Government at the destination specified in the contract, if transportation is f.o.b. destination.

(k) *Taxes*. The contract price includes all applicable Federal, State, and local taxes and duties.

(l) *Termination for the Government's convenience*. The Government reserves the right to terminate this contract, or any part hereof, for its sole convenience. In the event of such termination, the Contractor shall immediately stop all work hereunder and shall immediately cause any and all of its suppliers and subcontractors to cease work. Subject to the terms of this contract, the Contractor shall be paid a percentage of the contract price reflecting the percentage of the work performed prior to the notice of termination, plus reasonable charges the Contractor can demonstrate to the satisfaction of the Government using its standard record keeping system, have resulted from the termination. The Contractor shall not be required to comply with the cost accounting standards or contract cost principles for this purpose. This paragraph does not give the Government any right to audit the Contractor's records. The Contractor shall not be paid for any work performed or costs incurred which reasonably could have been avoided.

(m) *Termination for cause*. The Government may terminate this contract, or any part hereof, for cause in the event of any default by the Contractor, or if the Contractor fails to comply with any contract terms and conditions, or fails to provide the Government, upon request, with adequate assurances of future performance. In the event of termination for cause, the Government shall not be liable to the Contractor for any amount for supplies or services not accepted, and the Contractor shall be liable to the Government for any and all rights and remedies provided by law. If it is determined that the Government improperly terminated this contract for default, such termination shall be deemed a termination for convenience.

(n) *Title*. Unless specified elsewhere in this contract, title to items furnished under this contract shall pass to the Government upon acceptance, regardless of when or where the Government takes physical possession.

(o) *Warranty*. The Contractor warrants and implies that the items delivered hereunder are merchantable and fit for use for the particular purpose described in this contract.

(p) *Limitation of liability*. Except as otherwise provided by an express warranty, the Contractor will not be liable to the Government for consequential damages resulting from any defect or deficiencies in accepted items.

(q) *Other compliances*. The Contractor shall comply with all applicable Federal, State and local laws, executive orders, rules and regulations applicable to its performance under this contract.

(r) *Compliance with laws unique to Government contracts*. The Contractor agrees to comply with 31 U.S.C. 1352 relating to limitations on the use of appropriated funds to influence certain Federal contracts; 18 U.S.C. 431 relating to officials not to benefit; 40 U.S.C. 3701, *et seq*., Contract Work Hours and Safety Standards Act; 41 U.S.C. 51-58, Anti-Kickback Act of 1986; 41 U.S.C. 265 and 10 U.S.C. 2409 relating to whistleblower protections; 49 U.S.C. 40118, Fly American; and 41 U.S.C. 423 relating to procurement integrity.

(s) *Order of precedence*. Any inconsistencies in this solicitation or contract shall be resolved by giving precedence in the following order:

(1) The schedule of supplies/services.

(2) The Assignments, Disputes, Payments, Invoice, Other Compliances, and Compliance with Laws Unique to Government Contracts paragraphs of this clause.

(3) The clause at 52.212-5.

(4) Addenda to this solicitation or contract, including any license agreements for computer software.

(5) Solicitation provisions if this is a solicitation.

(6) Other paragraphs of this clause.

(7) The Standard Form 1449.

(8) Other documents, exhibits, and attachments.

The specification.

(t) *Central Contractor Registration (CCR).*

(1) Unless exempted by an addendum to this contract, the Contractor is responsible during performance and through final payment of any contract for the accuracy and completeness of the data within the CCR database, and for any liability resulting from the Government's reliance on inaccurate or incomplete data. To remain registered in the CCR database after the initial registration, the Contractor is required to review and update on an annual basis from the date of initial registration or subsequent updates its information in the CCR database to ensure it is current, accurate and complete. Updating information in the CCR does not alter the terms and conditions of this contract and is not a substitute for a properly executed contractual document.

(2)

(i) If a Contractor has legally changed its business name, "doing business as" name, or division name (whichever is shown on the contract), or has transferred the assets used in performing the contract, but has not completed the necessary requirements regarding novation and change-of-name agreements in Subpart 42.12, the Contractor shall provide the responsible Contracting Officer a minimum of one business day's written notification of its intention to:

(A) Change the name in the CCR database;

(B) Comply with the requirements of Subpart 42.12 of the FAR;

(C) Agree in writing to the timeline and procedures specified by the responsible Contracting Officer. The Contractor must provide with the notification sufficient documentation to support the legally changed name.

(ii) If the Contractor fails to comply with the requirements of paragraph (t)(2)(i) of this clause, or fails to perform the agreement at paragraph (t)(2)(i)(C) of this clause, and, in the absence of a properly executed novation or change-of-name agreement, the CCR information that shows the Contractor to be other than the Contractor indicated in the contract will be considered to be incorrect information within the meaning of the "Suspension of Payment" paragraph of the electronic funds transfer (EFT) clause of this contract.

The Contractor shall not change the name or address for EFT payments or manual payments, as appropriate, in the CCR record to reflect an assignee for the purpose of assignment of claims (see FAR Subpart 32.8, Assignment of Claims). Assignees shall be separately registered in the CCR database. Information provided to the Contractor's CCR record that indicates payments, including those made by EFT, to an ultimate recipient other than that Contractor will be

considered to be incorrect information within the meaning of the "Suspension of payment" paragraph of the EFT clause of this contract.
Offerors and Contractors may obtain information on registration and annual confirmation requirements via the Internet at http://www.ccr.gov or by calling 1-888-227-2423, or 269-961-5757.

(End of Clause)

52.212-5 – Contract Terms and Conditions Required to Implement Statutes or Executive Orders – Commercial Items.

Contract Terms and Conditions Required to Implement Statutes or Executive Orders – Commercial Items (Feb 2008)

(a) The Contractor shall comply with the following Federal Acquisition Regulation (FAR) clauses, which are incorporated in this contract by reference, to implement provisions of law or Executive orders applicable to acquisitions of commercial items:

(1) 52.233-3, Protest After Award (AUG 1996) (31 U.S.C. 3553).

(2) 52.233-4, Applicable Law for Breach of Contract Claim (OCT 2004) (Pub. L. 108-77, 108-78).

(b) The Contractor shall comply with the FAR clauses in this paragraph (b) that the contracting officer has indicated as being incorporated in this contract by reference to implement provisions of law or Executive orders applicable to acquisitions of commercial items:

[Contracting Officer shall check as appropriate.]

_X__ (1) 52.203-6, Restrictions on Subcontractor Sales to the Government (Sep 2006), with Alternate I (Oct 1995)(41 U.S.C. 253g and 10 U.S.C. 2402).

___ (2) 52.219-3, Notice of Total HUBZone Set-Aside (Jan 1999)(15 U.S.C. 657a).

___ (3) 52.219-4, Notice of Price Evaluation Preference for HUBZone Small Business Concerns (Jul 2005) (if the offeror elects to waive the preference, it shall so indicate in its offer)(15 U.S.C. 657a).

___ (4) [Reserved]

___ (5) (i) 52.219-6, Notice of Total Small Business Aside (June 2003) (15 U.S.C. 644).

___ (ii) Alternate I (Oct 1995) of 52.219-6.

___ (iii) Alternate II (Mar 2004) of 52.219-6.

___ (6) (i) 52.219-7, Notice of Partial Small Business Set-Aside (June 2003)(15 U.S.C. 644).

___ (ii) Alternate I (Oct 1995) of 52.219-7.

___ (iii) Alternate II (Mar 2004) of 52.219-7.

___ (7) 52.219-8, Utilization of Small Business Concerns (May 2004) (15 U.S.C. 637(d)(2) and (3)).

___ (8) (i) 52.219-9, Small Business Subcontracting Plan (Nov 2007)(15 U.S.C. 637 (d)(4).)

___ (ii) Alternate I (Oct 2001) of 52.219-9.

___ (iii) Alternate II (Oct 2001) of 52.219-9.

_X__ (9) 52.219-14, Limitations on Subcontracting (Dec 1996)(15 U.S.C. 637(a)(14)).

___ (10) 52.219-16, Liquidated Damages—Subcontracting Plan (Jan 1999)(15 U.S.C. 637(d)(4)(F)(i)).

___ (11) (i) 52.219-23, Notice of Price Evaluation Adjustment for Small Disadvantaged Business Concerns (Sep 2005)(10 U.S.C. 2323) (if the offeror elects to waive the adjustment, it shall so indicate in its offer).

___ (ii) Alternate I (June 2003) of 52.219-23.

___ (12) 52.219-25, Small Disadvantaged Business Participation Program—Disadvantaged Status and Reporting (Oct 1999)(Pub. L. 103-355, section 7102, and 10 U.S.C. 2323).

___ (13) 52.219-26, Small Disadvantaged Business Participation Program—Incentive Subcontracting (Oct 2000)(Pub. L. 103-355, section 7102, and 10 U.S.C. 2323).

___ (14) 52.219-27, Notice of Total Service-Disabled Veteran-Owned Small Business Set-Aside (May 2004) (15 U.S.C. 657 f).

___ (15) 52.219-28, Post Award Small Business Program Rerepresentation (June 2007) (15 U.S.C. 632(a)(2)).

___ (16) 52.222-3, Convict Labor (June 2003)(E.O. 11755).

_X__ (17) 52.222-19, Child Labor—Cooperation with Authorities and Remedies (Feb 2008) (E.O. 13126).

_X__ (18) 52.222-21, Prohibition of Segregated Facilities (Feb 1999).

_X__ (19) 52.222-26, Equal Opportunity (Mar 2007)(E.O. 11246).

_X__ (20) 52.222-35, Equal Opportunity for Special Disabled Veterans, Veterans of the Vietnam Era, and Other Eligible Veterans (Sep 2006)(38 U.S.C. 4212).

_X__ (21) 52.222-36, Affirmative Action for Workers with Disabilities (Jun 1998)(29 U.S.C. 793).

___ (22) 52.222-37, Employment Reports on Special Disabled Veterans, Veterans of the Vietnam Era, and Other Eligible Veterans (Sep 2006)(38 U.S.C. 4212).

___ (23) 52.222-39, Notification of Employee Rights Concerning Payment of Union Dues or Fees (Dec 2004) (E.O. 13201).

___ (24) (i) 52.222-50, Combating Trafficking in Persons (Aug 2007) (Applies to all contracts).

___ (ii) Alternate I (Aug 2007) of 52.222-50.

___ (25) (i) 52.223-9, Estimate of Percentage of Recovered Material Content for EPA-Designated Products (Aug 2000)(42 U.S.C. 6962(c)(3)(A)(ii)).

___ (ii) Alternate I (Aug 2000) of 52.223-9 (42 U.S.C. 6962(i)(2)(C)).

___ (26) 52.223-15, Energy Efficiency in Energy-Consuming Products (Dec 2007) (42 U.S.C. 8259b).

___ (27) (i) 52.223-16, IEEE 1680 Standard for the Environmental Assessment of Personal Computer Products (Dec 2007) (E.O. 13423).

___ (ii) Alternate I (Dec 2007) of 52.223-16.

___ (28) 52.225-1, Buy American Act--Supplies (June 2003)(41 U.S.C. 10a-10d).

_X__ (29) (i) 52.225-3, Buy American Act –Free Trade Agreements – Israeli Trade Act (Aug 2007) (41 U.S.C. 10a-10d, 19 U.S.C. 3301 note, 19 U.S.C. 2112 note, Pub. L. 108-77, 108-78, 108-286, and 109-169).

___ (ii) Alternate I (Jan 2004) of 52.225-3.

___ (iii) Alternate II (Jan 2004) of 52.225-3.

___ (30) 52.225-5, Trade Agreements (Nov 2007) (19 U.S.C. 2501, *et seq.*, 19 U.S.C. 3301 note).

_X__ (31) 52.225-13, Restrictions on Certain Foreign Purchases (Feb 2006) (E.o.s, proclamations, and statutes administered by the Office of Foreign Assets Control of the Department of the Treasury).

___ (32) 52.226-4, Notice of Disaster or Emergency Area Set-Aside (Nov 2007) (42 U.S.C. 5150).

___ (33) 52.226-5, Restrictions on Subcontracting Outside Disaster or Emergency Area (Nov 2007) (42 U.S.C. 5150).

___ (34) 52.232-29, Terms for Financing of Purchases of Commercial Items (Feb 2002) (41 U.S.C. 255(f), 10 U.S.C. 2307(f)).

_X_ (35) 52.232.30, Installment Payments for Commercial Items (Oct 1995)(41 U.S.C. 255(f), 10 U.S.C. 2307(f)).

___ (36) 52.232-33, Payment by Electronic Funds Transfer—Central Contractor Registration (Oct. 2003)(31 U.S.C. 3332).

___ (37) 52.232-34, Payment by Electronic Funds Transfer—Other Than Central Contractor Registration (May 1999)(31 U.S.C. 3332).

___ (38) 52.232-36, Payment by Third Party (May 1999)(31 U.S.C. 3332).

_X_ (39) 52.239-1, Privacy or Security Safeguards (Aug 1996)(5 U.S.C. 552a).

___ (40) (i) 52.247-64, Preference for Privately Owned U.S.-Flag Commercial Vessels (Feb 2006)(46 U.S.C. Appx 1241(b) and 10 U.S.C. 2631).

___ (ii) Alternate I (Apr 2003) of 52.247-64.

(c) The Contractor shall comply with the FAR clauses in this paragraph (c), applicable to commercial services, that the Contracting Officer has indicated as being incorporated in this contract by reference to implement provisions of law or executive orders applicable to acquisitions of commercial items:

[*Contracting Officer check as appropriate.*]

___ (1) 52.222-41, Service Contract Act of 1965 (Nov 2007)(41 U.S.C. 351, *et seq.*).

___ (2) 52.222-42, Statement of Equivalent Rates for Federal Hires (May 1989)(29 U.S.C. 206 and 41 U.S.C. 351, *et seq.*).

___ (3) 52.222-43, Fair Labor Standards Act and Service Contract Act -- Price Adjustment (Multiple Year and Option Contracts) (Nov 2006)(29 U.S.C.206 and 41 U.S.C. 351, *et seq.*).

___ (4) 52.222-44, Fair Labor Standards Act and Service Contract Act -- Price Adjustment (Feb 2002)(29 U.S.C. 206 and 41 U.S.C. 351, *et seq.*).

___ (5) 52.222-51, Exemption from Application of the Service Contract Act to Contracts for Maintenance, Calibration, or Repair of Certain Equipment--Requirements (Nov 2007) (41 U.S.C. 351, et seq.).

___ (6) 52.222-53, Exemption from Application of the Service Contract Act to Contracts for Certain Services--Requirements (Nov 2007) (41 U.S.C. 351, et seq.).

___ (7) 52.237-11, Accepting and Dispensing of $1 Coin (Aug 2007)(31 U.S.C. 5112(p)(1)).

(d) *Comptroller General Examination of Record.* The Contractor shall comply with the provisions of this paragraph (d) if this contract was awarded using other than sealed bid, is in excess of the simplified acquisition threshold, and does not contain the clause at 52.215-2, Audit and Records -- Negotiation.

(1) The Comptroller General of the United States, or an authorized representative of the Comptroller General, shall have access to and right to examine any of the Contractor's directly pertinent records involving transactions related to this contract.

(2) The Contractor shall make available at its offices at all reasonable times the records, materials, and other evidence for examination, audit, or reproduction, until 3 years after final payment under this contract or for any shorter period specified in FAR Subpart 4.7, Contractor Records Retention, of the other clauses of this contract. If this contract is completely or partially terminated, the records relating to the work terminated shall be made available for 3 years after any resulting final termination settlement. Records relating to appeals under the disputes clause or to litigation or the settlement of claims arising under or relating to this contract shall be made available until such appeals, litigation, or claims are finally resolved.

(3) As used in this clause, records include books, documents, accounting procedures and practices, and other data, regardless of type and regardless of form. This does not require the Contractor to create or maintain any record that the Contractor does not maintain in the ordinary course of business or pursuant to a provision of law.

(e)

(1) Notwithstanding the requirements of the clauses in paragraphs (a), (b), (c) and (d) of this clause, the Contractor is not required to flow down any FAR clause, other than those in paragraphs (i) through (vii) of this paragraph in a subcontract for commercial items. Unless otherwise indicated below, the extent of the flow down shall be as required by the clause--

(i) 52.219-8, Utilization of Small Business Concerns (May 2004)(15 U.S.C. 637(d)(2) and (3)), in all subcontracts that offer further subcontracting opportunities. If the subcontract (except subcontracts to small business concerns) exceeds $550,000 ($1,000,000 for construction of any public facility), the subcontractor must include 52.219-8 in lower tier subcontracts that offer subcontracting opportunities.

(ii) 52.222-26, Equal Opportunity (Mar 2007)(E.O. 11246).

(iii) 52.222-35, Equal Opportunity for Special Disabled Veterans, Veterans of the Vietnam Era, and Other Eligible Veterans (Sep 2006)(38 U.S.C. 4212).

(iv) 52.222-36, Affirmative Action for Workers with Disabilities (June 1998)(29 U.S.C. 793).

(v) 52.222-39, Notification of Employee rights Concerning Payment of Union Dues or Fees (Dec 2004) (E.O. 13201).

(vi) 52.222-41, Service Contract Act of 1965, (Nov 2007), flow down required for all subcontracts subject to the Service Contract Act of 1965 (41 U.S.C. 351, *et seq.*)

(vii) 52.222-50, Combating Trafficking in Persons (Aug 2007) (22 U.S.C. 7104(g)). Flow down required in accordance with paragraph (f) of FAR clause 52.222-50.

(viii) 52.222-51, Exemption from Application of the Service Contract Act to Contracts for Maintenance, Calibration, or Repair of Certain Equipment--Requirements (Nov 2007) (41 U.S.C. 351, et seq.)

(ix) 52.222-53, Exemption from Application of the Service Contract Act to Contracts for Certain Services--Requirements (Nov 2007) (41 U.S.C. 351, et seq.)

(x) 52.247-64, Preference for Privately-Owned U.S. Flag Commercial Vessels (Feb 2006) (46 U.S.C. Appx 1241(b) and 10 U.S.C. 2631). Flow down required in accordance with paragraph (d) of FAR clause 52.247-64.

(2) While not required, the contractor may include in its subcontracts for commercial items a minimal number of additional clauses necessary to satisfy its contractual obligations.

(End of Clause)

Alternate I (Feb 2000). As prescribed in 12.301(b)(4), delete paragraph (d) from the basic clause, redesignate paragraph (e) as paragraph (d), and revise the reference to "paragraphs (a), (b), (c), or (d) of this clause" in the redesignated paragraph (d) to read "paragraphs (a), (b), and (c) of this clause".

[Class Deviation- 2001-O0002, Commercial Item Omnibus Clauses for Acquisitions Using the Standard Procurement System. This clause deviation is effective on May 1, 2004, and remains in effect until April 20, 2009, or until other wise rescinded. (2004-o0002)

FAR 52.212-5 CONTRACT TERMS AND CONDITIONS REQUIRED TO IMPLEMENT STATUTES OR EXECUTIVE ORDERS--COMMERCIAL ITEMS (Feb 2008) (DEVIATION)

(a) Comptroller General Examination of Record. The Contractor shall comply with the provisions of this paragraph (a) if this contract was awarded using other than sealed bid, is in excess of the simplified acquisition threshold, and does not contain the clause at 52.215-2, Audit and Records -- Negotiation.

(1) The Comptroller General of the United States, or an authorized representative of the Comptroller General, shall have access to and right to examine any of the Contractor's directly pertinent records involving transactions related to this contract.

(2) The Contractor shall make available at its offices at all reasonable times the records, materials, and other evidence for examination, audit, or reproduction, until 3 years after final payment under this contract or for any shorter period specified in FAR Subpart 4.7, Contractor Records Retention, of the other clauses of this contract. If this contract is completely or partially terminated, the records relating to the work terminated shall be made available for 3 years after any resulting final termination settlement. Records relating to appeals under the disputes clause or to litigation or the settlement of claims arising under or relating to this contract shall be made available until such appeals, litigation, or claims are finally resolved.

(3) As used in this clause, records include books, documents, accounting procedures and practices, and other data, regardless of type and regardless of form. This does not require the Contractor to create or maintain any record that the Contractor does not maintain in the ordinary course of business or pursuant to a provision of law.

(b)

(1) Notwithstanding the requirements of any other clause in this contract, the Contractor is not required to flow down any FAR clause, other than those in paragraphs (i) through (vii) of this paragraph in a subcontract for commercial items. Unless otherwise indicated below, the extent of the flow down shall be as required by the clause.

(i) 52.219-8, Utilization of Small Business Concerns (May 2004)(15 U.S.C. 637(d)(2) and (3)), in all subcontracts that offer further subcontracting opportunities. If the subcontract (except subcontracts to small business concerns) exceeds $550,000 ($1,000,000 for construction of any public facility), the subcontractor must include 52.219-8 in lower tier subcontracts that offer subcontracting opportunities.

(ii) 52.222-26, Equal Opportunity (Mar 2007)(E.O. 11246).

(iii) 52.222-35, Equal Opportunity for Special Disabled Veterans, Veterans of the Vietnam Era, and Other Eligible Veterans (Sep 2006)(38 U.S.C. 4212).

(iv) 52.222-36, Affirmative Action for Workers with Disabilities (June 1998)(29 U.S.C. 793).

(v) 52.222-39, Notification of Employee rights Concerning Payment of Union Dues or Fees (Dec 2004) (E.O. 13201).

(vi) 52.222-41, Service Contract Act of 1965, (Nov 2007), flow down required for all subcontracts subject to the Service Contract Act of 1965 (41 U.S.C. 351, *et seq.*)

(vii) 52.222-50, Combating Trafficking in Persons (Aug 2007) (22 U.S.C. 7104(g)). Flow down required in accordance with paragraph (f) of FAR clause 52.222-50.

(viii) 52.222-51, Exemption from Application of the Service Contract Act to Contracts for Maintenance, Calibration, or Repair of Certain Equipment--Requirements ``(Nov 2007)'' (41 U.S.C. 351, et seq.)
(ix) 52.222-53, Exemption from Application of the Service Contract Act to Contracts for Certain Services--Requirements ``(Nov 2007)'' (41 U.S.C. 351, et seq.)
(x) 52.247-64, Preference for Privately-Owned U.S. Flag Commercial Vessels (Feb 2006) (46 U.S.C. Appx 1241(b) and 10 U.S.C. 2631). Flow down required in accordance with paragraph (d) of FAR clause 52.247-64.

(2) While not required, the contractor may include in its subcontracts for commercial items a minimal number of additional clauses necessary to satisfy its contractual obligations.

(End of Clause)

52.212-1 – Instructions to Offerors – Commercial Items.

As prescribed in 12.301(b)(1), insert the following provision:

Instructions to Offerors – Commercial Items (Nov 2007)

(a) *North American Industry Classification System (NAICS) code and small business size standard.* The NAICS code and small business size standard for this acquisition appear in Block 10 of the solicitation cover sheet (SF 1449). However, the small business size standard for a concern which submits an offer in its own name, but which proposes to furnish an item which it did not itself manufacture, is 500 employees.

(b) *Submission of offers.* Submit signed and dated offers to the office specified in this solicitation at or before the exact time specified in this solicitation. Offers may be submitted on the SF 1449, letterhead stationery, or as otherwise specified in the solicitation. As a minimum, offers must show --

(1) The solicitation number;
(2) The time specified in the solicitation for receipt of offers;
(3) The name, address, and telephone number of the offeror;
(4) A technical description of the items being offered in sufficient detail to evaluate compliance with the requirements in the solicitation. This may include product literature, or other documents, if necessary;
(5) Terms of any express warranty;
(6) Price and any discount terms;
(7) "Remit to" address, if different than mailing address;
(8) A completed copy of the representations and certifications at FAR 52.212-3 (see FAR 52.212-3(l) for those representations and certifications that the offeror shall complete electronically);
(9) Acknowledgment of Solicitation Amendments;
(10) Past performance information, when included as an evaluation factor, to include recent and relevant contracts for the same or similar items and other references (including contract numbers, points of contact with telephone numbers and other relevant information); and
(11) If the offer is not submitted on the SF 1449, include a statement specifying the extent of agreement with all terms, conditions, and provisions included in the solicitation. Offers that fail to furnish required representations or information, or reject the terms and conditions of the solicitation may be excluded from consideration.

(c) *Period for acceptance of offers.* The offeror agrees to hold the prices in its offer firm for 30 calendar days from the date specified for receipt of offers, unless another time period is specified in an addendum to the solicitation.

(d) Product samples. When required by the solicitation, product samples shall be submitted at or prior to the time specified for receipt of offers. Unless otherwise specified in this solicitation, these samples shall be submitted at no expense to the Government, and returned at the sender's request and expense, unless they are destroyed during preaward testing.

(e) Multiple offers. Offerors are encouraged to submit multiple offers presenting alternative terms and conditions or commercial items for satisfying the requirements of this solicitation. Each offer submitted will be evaluated separately.

(f) Late submissions, modifications, revisions, and withdrawals of offers.

(1) Offerors are responsible for submitting offers, and any modifications, revisions, or withdrawals, so as to reach the Government office designated in the solicitation by the time specified in the solicitation. If no time is specified in the solicitation, the time for receipt is 4:30 p.m., local time, for the designated Government office on the date that offers or revisions are due.

(2)

(i) Any offer, modification, revision, or withdrawal of an offer received at the Government office designated in the solicitation after the exact time specified for receipt of offers is "late" and will not be considered unless it is received before award is made, the Contracting Officer determines that accepting the late offer would not unduly delay the acquisition; and—

(A) If it was transmitted through an electronic commerce method authorized by the solicitation, it was received at the initial point of entry to the Government infrastructure not later than 5:00 p.m. one working day prior to the date specified for receipt of offers; or

(B) There is acceptable evidence to establish that it was received at the Government installation designated for receipt of offers and was under the Government's control prior to the time set for receipt of offers; or

(C) If this solicitation is a request for proposals, it was the only proposal received.

(ii) However, a late modification of an otherwise successful offer, that makes its terms more favorable to the Government, will be considered at any time it is received and may be accepted.

(3) Acceptable evidence to establish the time of receipt at the Government installation includes the time/date stamp of that installation on the offer wrapper, other documentary evidence of receipt maintained by the installation, or oral testimony or statements of Government personnel.

(4) If an emergency or unanticipated event interrupts normal Government processes so that offers cannot be received at the Government office designated for receipt of offers by the exact time specified in the solicitation, and urgent Government requirements preclude amendment of the solicitation or other notice of an extension of the closing date, the time specified for receipt of offers will be deemed to be extended to the same time of day specified in the solicitation on the first work day on which normal Government processes resume.

(5) Offers may be withdrawn by written notice received at any time before the exact time set for receipt of offers. Oral offers in response to oral solicitations

may be withdrawn orally. If the solicitation authorizes facsimile offers, offers may be withdrawn via facsimile received at any time before the exact time set for receipt of offers, subject to the conditions specified in the solicitation concerning facsimile offers. An offer may be withdrawn in person by an offeror or its authorized representative if, before the exact time set for receipt of offers, the identity of the person requesting withdrawal is established and the person signs a receipt for the offer.

(g) *Contract award (not applicable to Invitation for Bids).* The Government intends to evaluate offers and award a contract without discussions with offerors. Therefore, the offeror's initial offer should contain the offeror's best terms from a price and technical standpoint. However, the Government reserves the right to conduct discussions if later determined by the Contracting Officer to be necessary. The Government may reject any or all offers if such action is in the public interest; accept other than the lowest offer; and waive informalities and minor irregularities in offers received.

(h) *Multiple awards.* The Government may accept any item or group of items of an offer, unless the offeror qualifies the offer by specific limitations. Unless otherwise provided in the Schedule, offers may not be submitted for quantities less than those specified. The Government reserves the right to make an award on any item for a quantity less than the quantity offered, at the unit prices offered, unless the offeror specifies otherwise in the offer.

(i) *Availability of requirements documents cited in the solicitation.*

(1)(i) The GSA Index of Federal Specifications, Standards and Commercial Item Descriptions, FPMR Part 101-29, and copies of specifications, standards, and commercial item descriptions cited in this solicitation may be obtained for a fee by submitting a request to--

GSA Federal Supply Service Specifications Section
Suite 8100
470 L'Enfant Plaza, SW
Washington, DC 20407
Telephone (202) 619-8925)
Facsimile (202 619-8978).

(ii) If the General Services Administration, Department of Agriculture, or Department of Veterans Affairs issued this solicitation, a single copy of specifications, standards, and commercial item descriptions cited in this solicitation may be obtained free of charge by submitting a request to the addressee in paragraph (i)(1)(i) of this provision. Additional copies will be issued for a fee.

(2) Most unclassified Defense specifications and standards may be downloaded from the following ASSIST websites—

(i) ASSIST (http://assist.daps.dla.mil).

(ii) Quick Search (http://assist.daps.dla.mil/quicksearch/)

(iii) ASSISTdocs.com (http://assistdocs.com).

(3) Documents not available from ASSIST may be ordered from the Department of Defense Single Stock Point (DoDSSP) by—

(i) Using the ASSIST Shopping Wizard (http://assist.daps.dla.mil/wizard);

(ii) Phoning the DoDSSP Customer Service Desk (215) 697-2179, Mon-Fri, 0730 to 1600 EST; or

(iii) Ordering from DoDSSP, Building 4 Section D, 700 Robbins Avenue, Philadelphia, PA 19111-5094, Telephone (215) 697/2197, Facsimile (215) 697-1462.

(4) Nongovernment (voluntary) standards must be obtained from the organization responsible for their preparation, publication, or maintenance.

(j) *Data Universal Numbering System (DUNS) Number.* (Applies to offers exceeding $3,000, and offers of $3,000 or less if the solicitation requires the Contractor to be registered in the Central Contractor Registration (CCR) database. The offeror shall enter, in the block with its name and address on the cover page of its offer, the annotation "DUNS" or "DUNS+4" followed by the DUNS or DUNS+4 number that identifies the offeror's name and address. The DUNS+4 is the DUNS number plus a 4-character suffix that may be assigned at the discretion of the offeror to establish additional CCR records for identifying alternative Electronic Funds Transfer (EFT) accounts (see FAR Subpart 32.11) for the same parent concern. If the offeror does not have a DUNS number, it should contact Dun and Bradstreet directly to obtain one. An offeror within the United States may contact Dun and Bradstreet by calling 1-866-705-5711 or via the Internet at http://www.dnb.com. An offeror located outside the United States must contact the local Dun and Bradstreet office for DUNS number.

(k) *Central Contractor Registration.* Unless exempted by an addendum to this solicitation, by submission of an offer, the offeror acknowledges the requirement that a prospective awardee shall be registered in the CCR database prior to award, during performance and through final payment of any contract resulting from this solicitation. If the Offeror does not become registered in the CCR database in the time prescribed by the Contracting Officer, the Contracting Officer will proceed to award to the next otherwise successful registered Offeror. Offerors may obtain information on registration and annual confirmation requirements via the Internet at http://www.ccr.gov or by calling 1-888-227-2423 or 269-961-5757.

(l) *Debriefing.* If a post-award debriefing is given to requesting offerors, the Government shall disclose the following information, if applicable:

(1) The agency's evaluation of the significant weak or deficient factors in the debriefed offeror's offer.

(2) The overall evaluated cost or price and technical rating of the successful and debriefed offeror and past performance information on the debriefed offeror.

(3) The overall ranking of all offerors, when any ranking was developed by the agency during source selection.

(4) A summary of rationale for award;

(5) For acquisitions of commercial items, the make and model of the item to be delivered by the successful offeror.

(6) Reasonable responses to relevant questions posed by the debriefed offeror as to whether source-selection procedures set forth in the solicitation, applicable regulations, and other applicable authorities were followed by the agency.

(End of Provision)

52.212-3 – Offeror Representations and Certifications – Commercial Items (Nov 2007)

An offeror shall complete only paragraph (l) of this provision if the offeror has completed the annual representations and certificates electronically at http://orca.bpn.gov . If an offeror has not completed the annual representations and certifications electronically at the ORCA website, the offeror shall complete only paragraphs (b) through (k) of this provision.

(a) *Definitions.* As used in this provision--

"Emerging small business" means a small business concern whose size is no greater than 50 percent of the numerical size standard for the NAICS code designated.

"Forced or indentured child labor" means all work or service—

(1) Exacted from any person under the age of 18 under the menace of any penalty for its nonperformance and for which the worker does not offer himself voluntarily; or

(2) Performed by any person under the age of 18 pursuant to a contract the enforcement of which can be accomplished by process or penalties.

"Manufactured end product" means any end product in Federal Supply Classes (FSC) 1000-9999, except—

(1) FSC 5510, Lumber and Related Basic Wood Materials;
(2) Federal Supply Group (FSG) 87, Agricultural Supplies;
(3) FSG 88, Live Animals;
(4) FSG 89, Food and Related Consumables;
(5) FSC 9410, Crude Grades of Plant Materials;
(6) FSC 9430, Miscellaneous Crude Animal Products, Inedible;
(7) FSC 9440, Miscellaneous Crude Agricultural and Forestry Products;
(8) FSC 9610, Ores;
(9) FSC 9620, Minerals, Natural and Synthetic; and
(10) FSC 9630, Additive Metal Materials.

"Place of manufacture" means the place where an end product is assembled out of components, or otherwise made or processed from raw materials into the finished product that is to be provided to the Government. If a product is disassembled and reassembled, the place of reassembly is not the place of manufacture.

"Service-disabled veteran-owned small business concern"—

(1) Means a small business concern—

(i) Not less than 51 percent of which is owned by one or more service-disabled veterans or, in the case of any publicly owned business, not less than 51 percent of the stock of which is owned by one or more service-disabled veterans; and

(ii) The management and daily business operations of which are controlled by one or more service-disabled veterans or, in the case of a service-disabled veteran with permanent and severe disability, the spouse or permanent caregiver of such veteran.

(2) Service-disabled veteran means a veteran, as defined in 38 U.S.C. 101(2), with a disability that is service-connected, as defined in 38 U.S.C. 101(16).

"Small business concern" means a concern, including its affiliates, that is independently owned and operated, not dominant in the field of operation in which it is bidding on Government contracts, and qualified as a small business under the criteria in 13 CFR Part 121 and size standards in this solicitation.

"Veteran-owned small business concern" means a small business concern—

(1) Not less than 51 percent of which is owned by one or more veterans(as defined at 38 U.S.C. 101(2)) or, in the case of any publicly owned business, not less than 51 percent of the stock of which is owned by one or more veterans; and

(2) The management and daily business operations of which are controlled by one or more veterans.

"Women-owned business concern" means a concern which is at least 51 percent owned by one or more women; or in the case of any publicly owned business, at least 51 percent of the its stock is owned by one or more women; and whose management and daily business operations are controlled by one or more women.

"Women-owned small business concern" means a small business concern --

(1) That is at least 51 percent owned by one or more women or, in the case of any publicly owned business, at least 51 percent of the stock of which is owned by one or more women; and

(2) Whose management and daily business operations are controlled by one or more women.

(b) *Taxpayer identification number (TIN) (26 U.S.C. 6109, 31 U.S.C. 7701).* (Not applicable if the offeror is required to provide this information to a central contractor registration database to be eligible for award.)

(1) All offerors must submit the information required in paragraphs (b)(3) through (b)(5) of this provision to comply with debt collection requirements of 31 U.S.C. 7701(c) and 3325(d), reporting requirements of 26 U.S.C. 6041, 6041A, and 6050M, and implementing regulations issued by the Internal Revenue Service (IRS).

(2) The TIN may be used by the government to collect and report on any delinquent amounts arising out of the offeror's relationship with the Government (31 U.S.C. 7701(c)(3)). If the resulting contract is subject to the payment reporting requirements described in FAR 4.904, the TIN provided hereunder may be matched with IRS records to verify the accuracy of the offeror's TIN.]

(3) Taxpayer Identification Number (TIN).

* TIN:____________________.

* TIN has been applied for.

* TIN is not required because:

* Offeror is a nonresident alien, foreign corporation, or foreign partnership that does not have income effectively connected with the conduct of a trade or business in the United States and does not have an office or place of business or a fiscal paying agent in the United States;

* Offeror is an agency or instrumentality of a foreign government;

* Offeror is an agency or instrumentality of the Federal Government;

(4) Type of organization.

* Sole proprietorship;

* Partnership;

* Corporate entity (not tax-exempt);

* Corporate entity (tax-exempt);
* Government entity (Federal, State, or local);
* Foreign government;
* International organization per 26 CFR 1.6049-4;
* Other ____________________.

(5) Common parent.
* Offeror is not owned or controlled by a common parent:
* Name and TIN of common parent:
Name ___________________________________
TIN _____________________________________

(c) Offerors must complete the following representations when the resulting contract is to be performed in the United States or its outlying areas. Check all that apply.

(1) *Small business concern.* The offeror represents as part of its offer that it * is, * is not a small business concern.

(2) Veteran-owned small business concern. [Complete only if the offeror represented itself as a small business concern in paragraph (c)(1) of this provision.] The offeror represents as part of its offer that it * is, * is not a veteran-owned small business concern.

(3) Service-disabled veteran-owned small business concern. [Complete only if the offeror represented itself as a veteran-owned small business concern in paragraph (c)(2) of this provision.] The offeror represents as part of its offer that it * is, * is not a service-disabled veteran-owned small business concern.

(4) Small disadvantaged business concern. [Complete only if the offeror represented itself as a small business concern in paragraph (c)(1) of this provision.] The offeror represents, for general statistical purposes, that it * is, * is not, a small disadvantaged business concern as defined in 13 CFR 124.1002.

(5) Women-owned small business concern. [Complete only if the offeror represented itself as a small business concern in paragraph (c)(1) of this provision.] The offeror represents that it * is, * is not a women-owned small business concern.

Note: Complete paragraphs (c)(6) and (c)(7) only if this solicitation is expected to exceed the simplified acquisition threshold.

(6) Women-owned business concern (other than small business concern). [Complete only if the offeror is a women-owned business concern and did not represent itself as a small business concern in paragraph (c)(1) of this provision.]. The offeror represents that it * is, a women-owned business concern.

(7) *Tie bid priority for labor surplus area concerns.* If this is an invitation for bid, small business offerors may identify the labor surplus areas in which costs to be incurred on account of manufacturing or production (by offeror or first-tier subcontractors) amount to more than 50 percent of the contract price:

____

(8) Small Business Size for the Small Business Competitiveness Demonstration Program and for the Targeted Industry Categories under the Small Business Competitiveness Demonstration Program. *[Complete only if the offeror has represented itself to be a small business concern under the size standards for this solicitation.]*

(i) [*Complete only for solicitations indicated in an addendum as being set-aside for emerging small businesses in one of the designated industry* *groups (DIGs).*] The offeror represents as part of its offer that it * is, * is not an emerging small business.

(ii) [*Complete only for solicitations indicated in an addendum as being for one of the targeted industry categories (TICs) or designated industry groups (DIGs).*] Offeror represents as follows:

(A) Offeror's number of employees for the past 12 months (check the Employees column if size standard stated in the solicitation is expressed in terms of number of employees); or

(B) Offeror's average annual gross revenue for the last 3 fiscal years (check the Average Annual Gross Number of Revenues column if size standard stated in the solicitation is expressed in terms of annual receipts).

(Check one of the following):

Number of Employees	**Average Annual Gross Revenues**
50 or fewer	$1 million or less
51-100	$1,000,001-$2 million
101-250	$2,000,001-$3.5 million
251-500	$3,500,001-$5 million
501-750	$5,000,001-$10 million
751-1,000	$10,000,001-$17 million
Over 1,000	Over $17 million

(9) [Complete only if the solicitation contains the clause at FAR 52.219-23, Notice of Price Evaluation Adjustment for Small Disadvantaged Business Concerns, or FAR 52.219-25, Small Disadvantaged Business Participation Program—Disadvantaged Status and Reporting, and the offeror desires a benefit based on its disadvantaged status.]

(i) *General.* The offeror represents that either—

(A) It * is, * is not certified by the Small Business Administration as a small disadvantaged business concern and identified, on the date of this representation, as a certified small disadvantaged business concern in the database maintained by the Small Business Administration (PRO-Net), and that no material change in disadvantaged ownership and control has occurred since its certification, and, where the concern is owned by one or more individuals claiming disadvantaged status, the net worth of each individual upon whom the certification is based does not exceed $750,000 after taking into account the applicable exclusions set forth at 13 CFR 124.104(c)(2); or

(B) It *has, * has not submitted a completed application to the Small Business Administration or a Private Certifier to be certified as a small disadvantaged business concern in accordance with 13 CFR 124, Subpart B, and a decision on that application is pending, and that no material change in disadvantaged ownership and control has occurred since its application was submitted.

(ii) *Joint Ventures under the Price Evaluation Adjustment for Small Disadvantaged Business Concerns.* The offeror represents, as part of its offer, that it is a joint venture that complies with the requirements in 13 CFR 124.1002(f) and that the representation in paragraph (c)(9)(i) of this provision is accurate for the small disadvantaged business concern that is participating in the joint venture. [*The offeror shall enter the name of the small disadvantaged business concern that is participating in the joint venture:* ________________.]

(10) HUBZone small business concern. [Complete only if the offeror represented itself as a small business concern in paragraph (c)(1) of this provision.] The offeror represents, as part of its offer, that--

(i) It * is, * is not a HUBZone small business concern listed, on the date of this representation, on the List of Qualified HUBZone Small Business Concerns maintained by the Small Business Administration, and no material change in ownership and control, principal office, or HUBZone employee percentage has occurred since it was certified by the Small Business Administration in accordance with 13 CFR part 126; and

(ii) It * is, * not a joint venture that complies with the requirements of 13 CFR part 126, and the representation in paragraph (c)(10)(i) of this provision is accurate for the HUBZone small business concern or concerns that are participating in the joint venture. [*The offeror shall enter the name or names of the HUBZone small business concern or concerns that are participating in the joint venture*: __________.] Each HUBZone small business concern participating in the joint venture shall submit a separate signed copy of the HUBZone representation.

(d) *Representations required to implement provisions of Executive Order 11246* --

(1) Previous contracts and compliance. The offeror represents that --

(i) It * has, * has not, participated in a previous contract or subcontract subject to the Equal Opportunity clause of this solicitation; and

(ii) It * has, * has not, filed all required compliance reports.

(2) *Affirmative Action Compliance.* The offeror represents that --

(i) It * has developed and has on file, * has not developed and does not have on file, at each establishment, affirmative action programs required by rules and regulations of the Secretary of Labor (41 CFR parts 60-1 and 60-2), or

(ii) It * has not previously had contracts subject to the written affirmative action programs requirement of the rules and regulations of the Secretary of Labor.

(e) *Certification Regarding Payments to Influence Federal Transactions* (31 U.S.C. 1352). (Applies only if the contract is expected to exceed $100,000.) By submission of its offer, the offeror certifies to the best of its knowledge and belief that no Federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress or an employee of a Member of Congress on his or her behalf in connection with the award of any resultant contract. If any registrants under the Lobbying Disclosure Act of 1995 have made a lobbying contact on behalf of the offeror with respect to this contract, the offeror shall complete and submit, with its offer, OMB Standard Form LLL, Disclosure of Lobbying Activities, to provide the name of the registrants. The offeror need not report regularly employed officers or employees of the offeror to whom payments of reasonable compensation were made.

(f) *Buy American Act Certificate.* (Applies only if the clause at Federal Acquisition Regulation (FAR) 52.225-1, Buy American Act – Supplies, is included in this solicitation.)

(1) The offeror certifies that each end product, except those listed in paragraph (f)(2) of this provision, is a domestic end product and that the offeror has considered components of unknown origin to have been mined, produced, or manufactured outside the United States. The offeror shall list as foreign end products those end products manufactured in the United States that do not qualify as domestic end products. The terms "component," "domestic end product," "end product," "foreign end product," and "United States" are defined in the clause of this solicitation entitled "Buy American Act—Supplies."

(2) Foreign End Products:

LINE ITEM NO.	COUNTRY OF ORIGIN

[List as necessary]

(3) The Government will evaluate offers in accordance with the policies and procedures of FAR Part 25.

(g)

(1) *Buy American Act -- Free Trade Agreements -- Israeli Trade Act Certificate.* (Applies only if the clause at FAR 52.225-3, Buy American Act -- Free Trade Agreements -- Israeli Trade Act, is included in this solicitation.)

(i) The offeror certifies that each end product, except those listed in paragraph (g)(1)(ii) or (g)(1)(iii) of this provision, is a domestic end product and that the offeror has considered components of unknown origin to have been mined, produced, or manufactured outside the United States. The terms "Bahrainian or Moroccan end product," "component," "domestic end product," "end product," "foreign end product," "Free Trade Agreement country," "Free Trade Agreement country end product," "Israeli end product," and 'United States' are defined in the clause of this solicitation entitled "Buy American Act--Free Trade Agreements--Israeli Trade Act."

(ii) The offeror certifies that the following supplies are Free Trade Agreement country end products (other than Bahrainian or Moroccan end products) or Israeli end products as defined in the clause of this solicitation entitled "Buy American Act—Free Trade Agreements—Israeli Trade Act":

Free Trade Agreement Country End Products (Other than Bahrainian or Moroccan End Products) or Israeli End Products:

LINE ITEM NO.	COUNTRY OF ORIGIN

[List as necessary]

(iii) The offeror shall list those supplies that are foreign end products (other than those listed in paragraph (g)(1)(ii) or this provision) as defined in the clause of this solicitation entitled "Buy American Act—Free Trade Agreements—Israeli Trade Act." The offeror shall list as other foreign end products those end products manufactured in the United States that do not qualify as domestic end products.

Other Foreign End Products:

LINE ITEM NO.	COUNTRY OF ORIGIN

[List as necessary]

(iv) The Government will evaluate offers in accordance with the policies and procedures of FAR Part 25.

(2) *Buy American Act—Free Trade Agreements—Israeli Trade Act Certificate, Alternate I.* If Alternate I to the clause at FAR 52.225-3 is included in this solicitation, substitute the following paragraph (g)(1)(ii) for paragraph (g)(1)(ii) of the basic provision:

(g)(1)(ii) The offeror certifies that the following supplies are Canadian end products as defined in the clause of this solicitation entitled "Buy American Act—Free Trade Agreements—Israeli Trade Act":

Canadian End Products:

Line Item No.:

____

[List as necessary]

(3) *Buy American Act—Free Trade Agreements—Israeli Trade Act Certificate, Alternate II.* If Alternate II to the clause at FAR 52.225-3 is included in this solicitation, substitute the following paragraph (g)(1)(ii) for paragraph (g)(1)(ii) of the basic provision:

(g)(1)(ii) The offeror certifies that the following supplies are Canadian end products or Israeli end products as defined in the clause of this solicitation entitled ``Buy American Act--Free Trade Agreements--Israeli Trade Act":

Canadian or Israeli End Products:

Line Item No.:	Country of Origin:

[*List as necessary*]

(4) *Trade Agreements Certificate.* (Applies only if the clause at FAR 52.225-5, Trade Agreements, is included in this solicitation.)

(i) The offeror certifies that each end product, except those listed in paragraph (g)(4)(ii) of this provision, is a U.S.-made or designated country end product as defined in the clause of this solicitation entitled "Trade Agreements."

(ii) The offeror shall list as other end products those end products that are not U.S.-made or designated country end products.

Other End Products

Line Item No.:	Country of Origin:

[*List as necessary*]

(iii) The Government will evaluate offers in accordance with the policies and procedures of FAR Part 25. For line items covered by the WTO GPA, the Government will evaluate offers of U.S.-made or designated country end products without regard to the restrictions of the Buy American Act. The Government will consider for award only offers of U.S.-made or designated country end products unless the Contracting Officer determines that there are no offers for such products or that the offers for such products are insufficient to fulfill the requirements of the solicitation.

(h) *Certification Regarding Debarment, Suspension or Ineligibility for Award (Executive Order 12689).* (Applies only if the contract value is expected to exceed the simplified acquisition threshold.) The offeror certifies, to the best of its knowledge and belief, that the offeror and/or any of its principals–

(1) * Are, * are not presently debarred, suspended, proposed for debarment, or declared ineligible for the award of contracts by any Federal agency; and

(2) * Have, * have not, within a three-year period preceding this offer, been convicted of or had a civil judgment rendered against them for: commission of fraud or a criminal offense in connection with obtaining, attempting to obtain, or performing a Federal, state or local government contract or subcontract; violation of Federal or state antitrust statutes relating to the submission of offers; or commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, tax evasion, or receiving stolen property; and

(3) * Are, * are not presently indicted for, or otherwise criminally or civilly charged by a Government entity with, commission of any of these offenses.

(i) *Certification Regarding Knowledge of Child Labor for Listed End Products (Executive Order 13126). [The Contracting Officer must list in paragraph (i)(1) any end products being acquired under this solicitation that are included in the List of Products Requiring Contractor Certification as to Forced or Indentured Child Labor, unless excluded at 22.1503(b).]*

(1) Listed End Product

Listed End Product:	Listed Countries of Origin:

(2) Certification. [If the Contracting Officer has identified end products and countries of origin in paragraph (i)(1) of this provision, then the offeror must certify to either (i)(2)(i) or (i)(2)(ii) by checking the appropriate block.]

[ ] (i) The offeror will not supply any end product listed in paragraph (i)(1) of this provision that was mined, produced, or manufactured in the corresponding country as listed for that product.

[ ] (ii) The offeror may supply an end product listed in paragraph (i)(1) of this provision that was mined, produced, or manufactured in the corresponding country as listed for that product. The offeror certifies that is has made a good faith effort to determine whether forced or indentured child labor was used to mine, produce, or manufacture any such end product furnished under this contract. On the basis of those efforts, the offeror certifies that it is not aware of any such use of child labor.

(j) *Place of manufacture.* (Does not apply unless the solicitation is predominantly for the acquisition of manufactured end products.) For statistical purposes only, the offeror shall indicate whether the place of manufacture of the end products it expects to provide in response to this solicitation is predominantly—

(1) [ ] In the United States (Check this box if the total anticipated price of offered end products manufactured in the United States exceeds the total anticipated price of offered end products manufactured outside the United States); or

(2) [ ] Outside the United States.

(k) Certificates regarding exemptions from the application of the Service Contract Act. (Certification by the offeror as to its compliance with respect to the contract also constitutes its certification as to compliance by its subcontractor if it subcontracts out the exempt services.) [The contracting officer is to check a box to indicate if paragraph (k)(1) or (k)(2) applies.]

(1) [ ] Maintenance, calibration, or repair of certain equipment as described in FAR 22.1003-4(c)(1). The offeror [ ] does [ ] does not certify that—

(i) The items of equipment to be serviced under this contract are used regularly for other than Governmental purposes and are sold or traded by the offeror in substantial quantities to the general public in the course of normal business operations;

(ii) The services will be furnished at prices which are, or are based on, established catalog or market prices (see FAR 22.1003-4(c)(2)(ii)) for the maintenance, calibration, or repair of such equipment; and

(iii) The compensation (wage and fringe benefits) plan for all service employees performing work under the contract will be the same as that used for these employees and equivalent employees servicing the same equipment of commercial customers.

(2) [ ] Certain services as described in FAR 22.1003-4(d)(1). The offeror [ ] does [ ] does not certify that—

(i) The services under the contract are offered and sold regularly to non-Governmental customers, and are provided by the offeror (or subcontractor in the case of an exempt subcontract) to the general public in substantial quantities in the course of normal business operations;
(ii) The contract services will be furnished at prices that are, or are based on, established catalog or market prices (see FAR 22.1003-4(d)(2)(iii));
(iii) Each service employee who will perform the services under the contract will spend only a small portion of his or her time (a monthly average of less than 20 percent of the available hours on an annualized basis, or less than 20 percent of available hours during the contract period if the contract period is less than a month) servicing the Government contract; and
(iv) The compensation (wage and fringe benefits) plan for all service employees performing work under the contract is the same as that used for these employees and equivalent employees servicing commercial customers.

(3) If paragraph (k)(1) or (k)(2) of this clause applies—

(i) If the offeror does not certify to the conditions in paragraph (k)(1) or (k)(2) and the Contracting Officer did not attach a Service Contract Act wage determination to the solicitation, the offeror shall notify the Contracting Officer as soon as possible; and
(ii) The Contracting Officer may not make an award to the offeror if the offeror fails to execute the certification in paragraph (k)(1) or (k)(2) of this clause or to contact the Contracting Officer as required in paragraph (k)(3)(i) of this clause.

(l)

(1) *Annual Representations and Certifications.* Any changes provided by the offeror in paragraph (l)(2) of this provision do not automatically change the representations and certifications posted on the Online Representations and Certifications Application (ORCA) website.

(2) The offeror has completed the annual representations and certifications electronically via the ORCA website at http://orca.bpn.gov .After reviewing the ORCA database information, the offeror verifies by submission of this offer that the representation and certifications currently posted electronically at FAR 52.212-3, Offeror Representations and certifications—Commercial Items, have been entered or updated in the last 12 months, are current, accurate, complete, and applicable to this solicitation (including the business size standard applicable to the NAICS code referenced for this solicitation), as of the date of this offer and are incorporated in this offer by reference (see FAR 4.1201), except for paragraphs ____________. *[Offeror to identify the applicable paragraphs at (b) through (k) of this provision that the offeror has completed for the purposes of this solicitation only, if any. These amended representation(s) and/or certification(s) are also incorporated in this offer and are current, accurate, and complete as of the date of this offer. Any changes provided by the offeror are*

applicable to this solicitation only, and do not result in an update to the representations and certifications posted on ORCA.]

(End of Provision)

Alternate I (Apr 2002). As prescribed in 12.301(b)(2), add the following paragraph (c)(11) to the basic provision:

(11) (Complete if the offeror has represented itself as disadvantaged in paragraph (c)(4) or (c)(9) of this provision.) [*The offeror shall check the category in which its ownership falls*]:

____ Black American.

___ Hispanic American.

___ Native American (American Indians, Eskimos, Aleuts, or Native Hawaiians).

___ Asian-Pacific American (persons with origins from Burma, Thailand, Malaysia, Indonesia, Singapore, Brunei, Japan, China, Taiwan, Laos, Cambodia (Kampuchea), Vietnam, Korea, The Philippines, U.S. Trust Territory or the Pacific Islands (Republic of Palau), Republic of the Marshall Islands, Federated States of Micronesia, the Commonwealth of the Northern Mariana Islands, Guam, Samoa, Macao, Hong Kong, Fiji, Tonga, Kiribati, Tuvalu, or Nauru).

___ Subcontinent Asian (Asian-Indian) American (persons with origins from India, Pakistan, Bangladesh, Sri Lanka, Bhutan, the Maldives Islands, or Nepal).

___ Individual/concern, other than one of the preceding.

Alternate II (Oct 2000). As prescribed in 12.301(b)(2), add the following paragraph (c)(9)(iii) to the basic provision:

(iii) Address. The offeror represents that its address __is, __ is not in a region for which a small disadvantaged business procurement mechanism is authorized and its address has not changed since its certification as a small disadvantaged business concern or submission of its application for certification. The list of authorized small disadvantaged business procurement mechanisms and regions is posted at http://www.arnet.gov/References/sdbadjustments.htm. The offeror shall use the list in effect on the date of this solicitation. "Address," as used in this provision, means the address of the offeror as listed on the Small Business Administration's register of small disadvantaged business concerns or the address on the completed application that the concern has submitted to the Small Business Administration or a Private Certifier in accordance with 13 CFR part 124, subpart B. For joint ventures, "address" refers to the address of the small disadvantaged business concern that is participating in the joint venture.

SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL ITEMS
OFFEROR TO COMPLETE BLOCKS 12, 17, 23, 24, & 30

1. REQUISITION NUMBER: E009701048A
PAGE 1 OF 35

2. CONTRACT NO: BBGCON1808C6700
3. AWARD/EFFECTIVE DATE:
4. ORDER NUMBER:
5. SOLICITATION NUMBER: BBGCON1808S6700
6. SOLICITATION ISSUE DATE: 04/02/0

7. FOR SOLICITATION INFORMATION CALL:
a. NAME: Berel Dorfman
b. TELEPHONE NUMBER (No collect calls): (b) (6)
8. OFFER DUE DATE/LOCAL TIME:

9. ISSUED BY — CODE: M/CON/CR

Broadcasting Board of Governors
International Broadcasting Bureau
Office of Contracts (M/CON)
Room 4700, Switzer Building
330 C Street (SW)
Washington DC 20237

10. THIS ACQUISITION IS
☒ UNRESTRICTED OR ☐ SET ASIDE: % FOR
☐ SMALL BUSINESS ☐ EMERGING SMALL BUSINESS
☐ HUBZONE SMALL BUSINESS
☐ SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS ☐ 8(A)
NAICS:
SIZE STANDARD:

11. DELIVERY FOR FOB DESTINATION UNLESS BLOCK IS MARKED
☐ SEE SCHEDULE

12. DISCOUNT TERMS: Net 30

☐ 13a. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700)
13b. RATING
14. METHOD OF SOLICITATION
☐ RFQ ☐ IFB ☐ RFP

15. DELIVER TO — CODE: E/TT-KD

Kelly DeYoe
Broadcasting Board of Governors
International Broadcasting Bureau
330 C Street, SW, Room 4239
Washington DC 20237

16. ADMINISTERED BY — CODE: M/CON/CR

Broadcasting Board of Governors
International Broadcasting Bureau
Office of Contracts (M/CON)
Room 4700, Switzer Building
330 C Street (SW)
Washington DC 20237

17a. CONTRACTOR/OFFEROR — CODE: 809211100 — FACILITY CODE:

THE TOR PROJECT, INC.
Attn: Andrew Lewman
122 Scott Circle
Dedham MA 02026

TELEPHONE NO. (b) (6)

18a. PAYMENT WILL BE MADE BY — CODE: CFO/A

Broadcasting Board of Governors
International Broadcasting Bureau
Office of Financial Operations
CFO/A, Room 1655
330 Independence Ave., S.W.
Washington, DC 20237

☐ 17b. CHECK IF REMITTANCE IS DIFFERENT AND PUT SUCH ADDRESS IN OFFER

18b. SUBMIT INVOICES TO ADDRESS SHOWN IN BLOCK 18a UNLESS BLOCK BELOW IS CHECKED ☐ SEE ADDENDUM

19. ITEM NO	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
	Tax ID Number: 20-8096820 DUNS Number: 809211100 Contractor shall provide enhancements to TOR software system to meet the requirements cited in the Agency's Statement of Work (SOW) attached hereto (Addendum A). Period of Performance: 04/18/2008 to 04/17/2009				
0001	C.2.1 Continued design and development of enhancements to the existing TOR Software, C.2.2 Continued ...				70,000.00

(Use Reverse and/or Attach Additional Sheets as Necessary)

25. ACCOUNTING AND APPROPRIATION DATA: 9568-08-0206-E009701048A
26. TOTAL AWARD AMOUNT *(For Govt. Use Only)*: $360,000.00

☐ 27a. SOLICITATION INCORPORATES BY REFERENCE FAR 52.212-1, 52.212-4. FAR 52.212-3 AND 52.212-5 ARE ATTACHED. ADDEND ☐ ARE ☐ ARE NOT ATTACHED
☒ 27b. CONTRACT/PURCHASE ORDER INCORPORATES BY REFERENCE FAR 52.212-4. FAR 52.212-5 IS ATTACHED. ADDENDA ☒ ARE ☐ ARE NOT ATTACHED

☒ 28. CONTRACTOR IS REQUIRED TO SIGN THIS DOCUMENT AND RETURN 1 COPIES TO ISSUING OFFICE. CONTRACTOR AGREES TO FURNISH AND DELIVER ALL ITEMS SET FORTH OR OTHERWISE IDENTIFIED ABOVE AND ON ANY ADDITIONAL SHEETS SUBJECT TO THE TERMS AND CONDITIONS SPECIFIED HEREIN.

☐ 29. AWARD OF CONTRACT REF. ______ OFFER DATED ______. YOUR OFFER ON SOLICITATION (BLOCK 5), INCLUDING ANY ADDITIONS OR CHANGES WHICH ARE SET FORTH HEREIN, IS ACCEPTED AS TO ITEMS:

30a. SIGNATURE OF OFFEROR/CONTRACTOR
31a. UNITED STATES OF AMERICA (SIGNATURE OF CONTRACTING OFFICER)

(b) (6)

30b. NAME AND TITLE OF SIGNER (Type or print): Andrew Lewman, Clerk & Treasurer
30c. DATE SIGNED: 2008-04-25
31b. NAME OF CONTRACTING OFFICER (Type or print): Herman Shaw
31c. DATE SIGNED: 4/29/08

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
	Contractor shall submit system architecture and technical design documentation for TOR enhancemnets for review by AR/CO. Obligated Amount: $70,000.00				
0002	C.2.3 Continue development and implementation of the bridge relay mechanism, C.2.4 Continue development and implementation of the bridge directory authority mechanism, C.2.12 Continued development and implementation to the bridge relay and bridge directory mechanism. Obligated Amount: $80,000.00				80,000.00
0003	C.2.5 Continue design and develop revisions to the TOR network protocols to hide network signature of TOR traffic. Obligated Amount: $20,000.00				20,000.00
0004	C.2.6 Continue to develop and implement enhancements to TOR's cell-based protocol, C.2.7 Continue development of TOR network scalability, and C.2.13 Research and document additional options for the scalability of the TOR network beyond 2 million concurrent users. Obligated Amount: $80,000.00 Continued ...				80,000.00

32a. QUANTITY IN COLUMN 21 HAS BEEN

□ RECEIVED □ INSPECTED □ ACCEPTED, AND CONFORMS TO THE CONTRACT, EXCEPT AS NOTED:

32b. SIGNATURE OF AUTHORIZED GOVERNMENT REPRESENTATIVE

32c. DATE

32d. PRINTED NAME AND TITLE OF AUTHORIZED GOVERNMENT REPRESENTATIVE

32e. MAILING ADDRESS OF AUTHORIZED GOVERNMENT REPRESENTATIVE

32f. TELEPHONE NUMBER OF AUTHORIZED GOVERNMENT REPRESENTATIVE

32g. E-MAIL OF AUTHORIZED GOVERNMENT REPRESENTATIVE

33. SHIP NUMBER

□ PARTIAL □ FINAL

34. VOUCHER NUMBER

35. AMOUNT VERIFIED CORRECT FOR

36. PAYMENT

□ COMPLETE □ PARTIAL □ FINAL

37. CHECK NUMBER

38. S/R ACCOUNT NUMBER

39. S/R VOUCHER NUMBER

40. PAID BY

41a. I CERTIFY THIS ACCOUNT IS CORRECT AND PROPER FOR PAYMENT

41b. SIGNATURE AND TITLE OF CERTIFYING OFFICER

41c. DATE

42a. RECEIVED BY *(Print)*

42b. RECEIVED AT *(Location)*

42c. DATE REC'D *(YY/MM/DD)*

42d. TOTAL CONTAINERS

CONTINUATION SHEET	REFERENCE NO. OF DOCUMENT BEING CONTINUED BBGCON1808C6700	PAGE 3	OF 35

NAME OF OFFEROR OR CONTRACTOR
THE TOR PROJECT, INC.

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
0005	C.2.8 Continue to work with IBB staff and other IBB contractors to identify tasks in support of this program, and C.2.9 Communicate tasks identified in C.2.8 to the AR/CO and negotiate time frames for their completion. Obligated Amount: $0.00				0.00
0006	C.2.10 Promote active growth of the TOR server network and advocacy of TOR products. Obligated Amount: $20,000.00				20,000.00
0007	C.2.11 Improve the ease of use of TOR for end users by continuing research and development. Obligated Amount: $20,000.00				20,000.00
0008	C.2.14 Continue reaserch into the option of providing incentives for TOR users to run TOR relay servers. Obligated Amount: $30,000.00				30,000.00
0009	C.2.15 Develop a more reliable download mechanism for the TOR browser bundle for users on slow and/or unreliable network connections. Obligated Amount: $10,000.00				10,000.00
0010	C.2.16 Test the TOR bundle browser in multiple computer systems and analyze these systems for any changes to the system that may have been made inadvertently by use of the TOR browser bundle. Obligated Amount: $10,000.00				10,000.00
0011	C.2.17 Develop or adapt existing open source software to implement a web-based portal to manage the translation of text into multiple languages for the user interface text or software or Torbutton and Vidalia and other software that may be included in the TOR web browser. Obligated Amount: $20,000.00				20,000.00
	Continued ...				

CONTINUATION SHEET	REFERENCE NO. OF DOCUMENT BEING CONTINUED BBGCON1808C6700	PAGE 4 OF 35

NAME OF OFFEROR OR CONTRACTOR
THE TOR PROJECT, INC.

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	The total amount of award: $360,000.00. The obligation for this award is shown in box 26.				

Addendum "A" – STATEMENT OF WORK

SECTION C

C.1 BACKGROUND

The Broadcasting Board of Governors (BBG) oversees the mission and operation of several overseas broadcasting entities of the United States Government (USG). The International Broadcasting Bureau (IBB) oversees the daily operations of several USG broadcasters, including the Voice of America (VOA), and is responsible for all contractual and fiscal matters pertaining to broadcast operations. The IBB's Internet anti-censorship program seeks to ensure Internet users in target countries are able to access USG broadcasters' web sites to access their news and other programming, using a variety of tools to counter foreign government-sponsored Internet censorship controls.

This Statement of Work defines those duties the Contractor shall perform to enable the IBB to meet its goals of using Tor as a tool to further its Internet anti-censorship efforts.

C.2 TECHNICAL REQUIREMENTS

C.2.1 The Contractor shall continue design and development of enhancements to the existing Tor software to increase its suitability as a tool for Internet users in countries with government-sponsored Internet censorship to circumvent censorship controls, based on the existing research and documentation performed during the previous contract period (e.g. as described in the paper "Design of a blocking-resistant anonymity system").

C.2.2 The Contractor shall submit system architecture and technical design documentation for Tor enhancements specifically related to anti-censorship improvements in C.2.1 to the Authorized Representative of the Contracting Officer (AR/CO) for review and approval before implementation. Significant changes to the design that are discovered during implementation must be documented and reviewed by the AR/CO as soon as the Contractor becomes aware of the need for these revisions.

C.2.3 The Contractor shall continue to develop and implement the bridge relay mechanism as designed during the previous contract period to allow individual Tor users to easily reconfigure their Tor client to automatically relay traffic from users in countries with government-imposed Internet censorship so as to circumvent that censorship.

C.2.4 The Contractor shall continue to develop and implement the bridge directory authority mechanism as designed during the previous contract period to allow Tor clients configured as bridge relays (as described in C.2.3) to communicate their existence to the bridge directory authority, and to allow users in countries with government-imposed Internet censorship to discover addresses of available bridge relays so that they may access the Tor network.

C.2.5 The Contractor shall design and develop revisions to the Tor network protocols to hide the network signature of Tor traffic so it is difficult for government-sponsored Internet censors to identify Tor traffic and trivially block it.

C.2.6 The Contractor shall continue to develop and implement enhancements to Tor's cell-based protocol to improve performance on substandard network connections including those with low bandwidth and/or high latency and/or high packet loss.

C.2.7 The Contractor shall continue development of Tor network scalability, with the goal of supporting 2 million or more concurrent end users. This requirement is only a goal for system scalability and is not a requirement on number of actual concurrent users of the Tor network.

C.2.8 The Contractor shall work with IBB staff and other IBB contractors to identify tasks in support of this program that might be developed collaboratively with Contractor. Tasks involving areas such as documentation, bug fixes, software testing, and any area where specific knowledge of foreign government-sponsored Internet censorship may be especially appropriate for this purpose.

C.2.9 The Contractor shall communicate tasks identified for delegation to IBB in C.2.8 to the AR/CO and negotiate time frames for their completion. The Contractor shall monitor and coordinate work performed by IBB staff on delegated tasks and integrate it into Tor software releases as appropriate.

C.2.10 The Contractor shall promote active growth of the Tor server network and advocacy of Tor products to increase the performance, stability, and usability of Tor, with a focus on the end user experience for users in countries with government-sponsored Internet censorship.

C.2.11 The Contractor shall improve the ease of use of Tor for end users by continuing research and development of one or both of the following products: (1) all-in-one software bundle containing Tor and supporting applications, as well as an easy-to-use installer for Microsoft Windows operating systems, as well as option to install and run from a Universal Serial Bus (USB) flash device; (2) bootable CD-ROM image ("LiveCD") which contains a minimal operating system, Tor, and supporting applications. Both would have all appropriate applications pre-configured to use Tor out of the box with only minimal additional configuration required by the end user. If Contractor determines it is not feasible to develop both products, Contractor will provide detailed written technical analysis and explanation to the AR/CO. The Contractor shall make an initial public release of at least one of these products during the term of this contract.

C.2.12 The Contractor shall continue to develop and implement improvements to the bridge relay and bridge directory authority mechanisms to improve the usability, performance and reliability of the Tor network by users in countries with government-imposed Internet censorship.

C.2.13 The Contractor shall research and document additional options for the scalability of the Tor network beyond 2 million concurrent users, including analysis of splitting the network into multiple segments, switching to datagram-based protocols, and improving the load balancing within the network.

C.2.14 The Contractor shall continue research into the option of providing incentives for Tor users to run Tor relay servers. If further research indicates that this should be pursued, the Contractor shall develop a project plan and timeline for this work. If further research indicates this option should be abandoned, the Contractor shall document and explain in writing the reasoning behind this decision.

C.2.15 The Contractor shall develop a more reliable download mechanism for the Tor browser bundle for users on slow and/or unreliable network connections, by means of a split download of multiple smaller files, implementation of a lightweight download manager, reduction in the software bundle file size, or other method as chosen by the Contractor.

C.2.16 The Contractor shall test the Tor browser bundle on multiple computer systems and analyze these systems afterwards for any changes to the system that may have been made inadvertently by use of the Tor browser bundle. The Contractor shall document any such changes found and develop a plan to reduce the footprint of Tor browser bundle use.

C.2.17 The Contractor shall develop or adapt existing open source software to implement a web-based portal to manage the translations of text into multiple languages for the user interface text of software of Torbutton and Vidalia and other software that may in the future be included in the Tor browser bundle. The web site must allow non-technical users the ability to contribute translations by providing text to be translated in English, as well as any needed context on the use of the text, and allowing users to enter the translation into their language from their web browser.

C.3 ADMINISTRATIVE REQUIREMENTS

C.3.1 The Contractor shall provide a Monthly Status Report within ten (10) business days of the end of the month to the AR/CO detailing work performed during the previous month. This report shall describe the work performed for specific requirements of this contract. The report shall also include any other relevant information on Tor activities that may have indirect impacts on contracted work.

C.3.2 The Contractor shall be available for a telephone conference call with the AR/CO, other IBB staff and representatives at a mutually agreeable time on a periodic basis averaging no more than 2 calls per month of one hour's duration. This requirement is in addition to any other required communication by telephone or email with the AR/CO for execution of this contract.

C.4 ADDITIONAL TERMS

C.4.1 All software and accompanying documentation developed under the terms of this contract must be distributed under an open source software license, such as the "BSD License" or other commonly accepted open source software license as mutually agreed upon by the Contractor and the AR/CO.

Addendum "B" – PRICING SCHEDULE

Item Number	Description	Fixed Price
C.2.1 & C.2.2	See SOW C.2.1 & C.2.2	$70,000
C.2.3, C.2.4, & C.2.12	See SOW C.2.3, C.2.4, & C.2.12	$80,000
C.2.5	See SOW C.2.5	$20,000
C.2.6, C.2.7, & C.2.13	See SOW C.2.6, C.2.7, & C.2.13	$80,000
C.2.8 & C.2.9	See SOW C.2.8 & C.2.9	$0
C.2.10	See SOW C.2.10	$20,000
C.2.11	See SOW C.2.11	$20,000
C.2.14	See SOW C.2.14	$30,000
C.2.15	See SOW C.2.15	$10,000
C.2.16	See SOW C.2.16	$10,000
C.2.17	See SOW C.2.17	$20,000

Total Firm Fixed Price contract $ 360,000

52.212-4 – Contract Terms and Conditions – Commercial Items.

As prescribed in 12.301(b)(3), insert the following clause:

Contract Terms and Conditions – Commercial Items (Feb 2007)

(a) *Inspection/Acceptance.* The Contractor shall only tender for acceptance those items that conform to the requirements of this contract. The Government reserves the right to inspect or test any supplies or services that have been tendered for acceptance. The Government may require repair or replacement of nonconforming supplies or reperformance of nonconforming services at no increase in contract price. If repair/replacement or reperformance will not correct the defects or is not possible, the government may seek an equitable price reduction or adequate consideration for acceptance of nonconforming supplies or services. The Government must exercise its post-acceptance rights --

(1) Within a reasonable time after the defect was discovered or should have been discovered; and

(2) Before any substantial change occurs in the condition of the item, unless the change is due to the defect in the item.

(b) *Assignment.* The Contractor or its assignee may assign its rights to receive payment due as a result of performance of this contract to a bank, trust company, or other financing institution, including any Federal lending agency in accordance with the Assignment of Claims Act (31 U.S.C.3727). However, when a third party makes payment (*e.g.*, use of the Governmentwide commercial purchase card), the Contractor may not assign its rights to receive payment under this contract.

(c) *Changes.* Changes in the terms and conditions of this contract may be made only by written agreement of the parties.

(d) *Disputes.* This contract is subject to the Contract Disputes Act of 1978, as amended (41 U.S.C. 601-613). Failure of the parties to this contract to reach agreement on any request for equitable adjustment, claim, appeal or action arising under or relating to this contract shall be a dispute to be resolved in accordance with the clause at FAR 52.233-1, Disputes, which is incorporated herein by reference. The Contractor shall proceed diligently with performance of this contract, pending final resolution of any dispute arising under the contract.

(e) *Definitions.* The clause at FAR 52.202-1, Definitions, is incorporated herein by reference.

(f) *Excusable delays.* The Contractor shall be liable for default unless nonperformance is caused by an occurrence beyond the reasonable control of the Contractor and without its fault or negligence such as, acts of God or the public enemy, acts of the Government in either its sovereign or contractual capacity, fires, floods, epidemics, quarantine restrictions, strikes, unusually severe weather, and delays of common carriers. The Contractor shall notify the Contracting Officer in writing as soon as it is reasonably possible after the commencement of any excusable delay, setting forth the full particulars in connection therewith, shall remedy such occurrence with all reasonable dispatch, and shall promptly give written notice to the Contracting Officer of the cessation of such occurrence.

(g) *Invoice.*

(1) The Contractor shall submit an original invoice and three copies (or electronic invoice, if authorized) to the address designated in the contract to receive invoices. An invoice must include --

(i) Name and address of the Contractor;

(ii) Invoice date and number;

(iii) Contract number, contract line item number and, if applicable, the order number;

(iv) Description, quantity, unit of measure, unit price and extended price of the items delivered;
(v) Shipping number and date of shipment, including the bill of lading number and weight of shipment if shipped on Government bill of lading;
(vi) Terms of any discount for prompt payment offered;
(vii) Name and address of official to whom payment is to be sent;
(viii) Name, title, and phone number of person to notify in event of defective invoice; and
(ix) Taxpayer Identification Number (TIN). The Contractor shall include its TIN on the invoice only if required elsewhere in this contract.
(x) Electronic funds transfer (EFT) banking information.

(A) The Contractor shall include EFT banking information on the invoice only if required elsewhere in this contract.
(B) If EFT banking information is not required to be on the invoice, in order for the invoice to be a proper invoice, the Contractor shall have submitted correct EFT banking information in accordance with the applicable solicitation provision, contract clause (*e.g.*, 52.232-33, Payment by Electronic Funds Transfer—Central Contractor Registration, or 52.232-34, Payment by Electronic Funds Transfer—Other Than Central Contractor Registration), or applicable agency procedures.
(C) EFT banking information is not required if the Government waived the requirement to pay by EFT.

(2) Invoices will be handled in accordance with the Prompt Payment Act (31 U.S.C. 3903) and Office of Management and Budget (OMB) prompt payment regulations at 5 CFR part 1315.

(h) *Patent indemnity*. The Contractor shall indemnify the Government and its officers, employees and agents against liability, including costs, for actual or alleged direct or contributory infringement of, or inducement to infringe, any United States or foreign patent, trademark or copyright, arising out of the performance of this contract, provided the Contractor is reasonably notified of such claims and proceedings.

(i) *Payment*.

(1) Items accepted. Payment shall be made for items accepted by the Government that have been delivered to the delivery destinations set forth in this contract.
(2) Prompt Payment. The Government will make payment in accordance with the Prompt Payment Act (31 U.S.C. 3903) and prompt payment regulations at 5 CFR Part 1315.
(3) Electronic Funds Transfer (EFT). If the Government makes payment by EFT, see 52.212-5(b) for the appropriate EFT clause.
(4) Discount. In connection with any discount offered for early payment, time shall be computed from the date of the invoice. For the purpose of computing the discount earned, payment shall be considered to have been made on the date which appears on the payment check or the specified payment date if an electronic funds transfer payment is made.
(5) Overpayments. If the Contractor becomes aware of a duplicate contract financing or invoice payment or that the Government has otherwise overpaid on a contract financing or invoice payment, the Contractor shall immediately notify the Contracting Officer and request instructions for disposition of the overpayment.

(j) *Risk of loss*. Unless the contract specifically provides otherwise, risk of loss or damage to the supplies provided under this contract shall remain with the Contractor until, and shall pass to the Government upon:

(1) Delivery of the supplies to a carrier, if transportation is f.o.b. origin; or

(2) Delivery of the supplies to the Government at the destination specified in the contract, if transportation is f.o.b. destination.

(k) *Taxes*. The contract price includes all applicable Federal, State, and local taxes and duties.

(l) *Termination for the Government's convenience*. The Government reserves the right to terminate this contract, or any part hereof, for its sole convenience. In the event of such termination, the Contractor shall immediately stop all work hereunder and shall immediately cause any and all of its suppliers and subcontractors to cease work. Subject to the terms of this contract, the Contractor shall be paid a percentage of the contract price reflecting the percentage of the work performed prior to the notice of termination, plus reasonable charges the Contractor can demonstrate to the satisfaction of the Government using its standard record keeping system, have resulted from the termination. The Contractor shall not be required to comply with the cost accounting standards or contract cost principles for this purpose. This paragraph does not give the Government any right to audit the Contractor's records. The Contractor shall not be paid for any work performed or costs incurred which reasonably could have been avoided.

(m) *Termination for cause*. The Government may terminate this contract, or any part hereof, for cause in the event of any default by the Contractor, or if the Contractor fails to comply with any contract terms and conditions, or fails to provide the Government, upon request, with adequate assurances of future performance. In the event of termination for cause, the Government shall not be liable to the Contractor for any amount for supplies or services not accepted, and the Contractor shall be liable to the Government for any and all rights and remedies provided by law. If it is determined that the Government improperly terminated this contract for default, such termination shall be deemed a termination for convenience.

(n) *Title*. Unless specified elsewhere in this contract, title to items furnished under this contract shall pass to the Government upon acceptance, regardless of when or where the Government takes physical possession.

(o) *Warranty*. The Contractor warrants and implies that the items delivered hereunder are merchantable and fit for use for the particular purpose described in this contract.

(p) *Limitation of liability*. Except as otherwise provided by an express warranty, the Contractor will not be liable to the Government for consequential damages resulting from any defect or deficiencies in accepted items.

(q) *Other compliances*. The Contractor shall comply with all applicable Federal, State and local laws, executive orders, rules and regulations applicable to its performance under this contract.

(r) *Compliance with laws unique to Government contracts*. The Contractor agrees to comply with 31 U.S.C. 1352 relating to limitations on the use of appropriated funds to influence certain Federal contracts; 18 U.S.C. 431 relating to officials not to benefit; 40 U.S.C. 3701, *et seq*., Contract Work Hours and Safety Standards Act; 41 U.S.C. 51-58, Anti-Kickback Act of 1986; 41 U.S.C. 265 and 10 U.S.C. 2409 relating to whistleblower protections; 49 U.S.C. 40118, Fly American; and 41 U.S.C. 423 relating to procurement integrity.

(s) *Order of precedence*. Any inconsistencies in this solicitation or contract shall be resolved by giving precedence in the following order:

(1) The schedule of supplies/services.

(2) The Assignments, Disputes, Payments, Invoice, Other Compliances, and Compliance with Laws Unique to Government Contracts paragraphs of this clause.

(3) The clause at 52.212-5.
(4) Addenda to this solicitation or contract, including any license agreements for computer software.
(5) Solicitation provisions if this is a solicitation.
(6) Other paragraphs of this clause.
(7) The Standard Form 1449.
(8) Other documents, exhibits, and attachments.
The specification.

(t) *Central Contractor Registration (CCR).*

(1) Unless exempted by an addendum to this contract, the Contractor is responsible during performance and through final payment of any contract for the accuracy and completeness of the data within the CCR database, and for any liability resulting from the Government's reliance on inaccurate or incomplete data. To remain registered in the CCR database after the initial registration, the Contractor is required to review and update on an annual basis from the date of initial registration or subsequent updates its information in the CCR database to ensure it is current, accurate and complete. Updating information in the CCR does not alter the terms and conditions of this contract and is not a substitute for a properly executed contractual document.

(2)

(i) If a Contractor has legally changed its business name, "doing business as" name, or division name (whichever is shown on the contract), or has transferred the assets used in performing the contract, but has not completed the necessary requirements regarding novation and change-of-name agreements in Subpart 42.12, the Contractor shall provide the responsible Contracting Officer a minimum of one business day's written notification of its intention to:

(A) Change the name in the CCR database;
(B) Comply with the requirements of Subpart 42.12 of the FAR;
(C) Agree in writing to the timeline and procedures specified by the responsible Contracting Officer. The Contractor must provide with the notification sufficient documentation to support the legally changed name.

(ii) If the Contractor fails to comply with the requirements of paragraph (t)(2)(i) of this clause, or fails to perform the agreement at paragraph (t)(2)(i)(C) of this clause, and, in the absence of a properly executed novation or change-of-name agreement, the CCR information that shows the Contractor to be other than the Contractor indicated in the contract will be considered to be incorrect information within the meaning of the "Suspension of Payment" paragraph of the electronic funds transfer (EFT) clause of this contract.

The Contractor shall not change the name or address for EFT payments or manual payments, as appropriate, in the CCR record to reflect an assignee for the purpose of assignment of claims (see FAR Subpart 32.8, Assignment of Claims). Assignees shall be separately registered in the CCR database. Information provided to the Contractor's CCR record that indicates payments, including those made by EFT, to an ultimate recipient other than that Contractor will be considered to be incorrect information within the meaning of the "Suspension of payment" paragraph of the EFT clause of this contract.

Offerors and Contractors may obtain information on registration and annual confirmation requirements via the Internet at http://www.ccr.gov or by calling 1-888-227-2423, or 269-961-5757.

(End of Clause)

52.212-5 – Contract Terms and Conditions Required to Implement Statutes or Executive Orders – Commercial Items.

Contract Terms and Conditions Required to Implement Statutes or Executive Orders – Commercial Items (Feb 2008)

(a) The Contractor shall comply with the following Federal Acquisition Regulation (FAR) clauses, which are incorporated in this contract by reference, to implement provisions of law or Executive orders applicable to acquisitions of commercial items:

(1) 52.233-3, Protest After Award (AUG 1996) (31 U.S.C. 3553).

(2) 52.233-4, Applicable Law for Breach of Contract Claim (OCT 2004) (Pub. L. 108-77, 108-78).

(b) The Contractor shall comply with the FAR clauses in this paragraph (b) that the contracting officer has indicated as being incorporated in this contract by reference to implement provisions of law or Executive orders applicable to acquisitions of commercial items:

[Contracting Officer shall check as appropriate.]

_X_ (1) 52.203-6, Restrictions on Subcontractor Sales to the Government (Sep 2006), with Alternate I (Oct 1995)(41 U.S.C. 253g and 10 U.S.C. 2402).

___ (2) 52.219-3, Notice of Total HUBZone Set-Aside (Jan 1999)(15 U.S.C. 657a).

___ (3) 52.219-4, Notice of Price Evaluation Preference for HUBZone Small Business Concerns (Jul 2005) (if the offeror elects to waive the preference, it shall so indicate in its offer)(15 U.S.C. 657a).

___ (4) [Reserved]

___ (5) (i) 52.219-6, Notice of Total Small Business Aside (June 2003) (15 U.S.C. 644).

___ (ii) Alternate I (Oct 1995) of 52.219-6.

___ (iii) Alternate II (Mar 2004) of 52.219-6.

___ (6) (i) 52.219-7, Notice of Partial Small Business Set-Aside (June 2003)(15 U.S.C. 644).

___ (ii) Alternate I (Oct 1995) of 52.219-7.

___ (iii) Alternate II (Mar 2004) of 52.219-7.

___ (7) 52.219-8, Utilization of Small Business Concerns (May 2004) (15 U.S.C. 637(d)(2) and (3)).

___ (8) (i) 52.219-9, Small Business Subcontracting Plan (Nov 2007)(15 U.S.C. 637 (d)(4).)

___ (ii) Alternate I (Oct 2001) of 52.219-9.

___ (iii) Alternate II (Oct 2001) of 52.219-9.

_X_ (9) 52.219-14, Limitations on Subcontracting (Dec 1996)(15 U.S.C. 637(a)(14)).

___ (10) 52.219-16, Liquidated Damages—Subcontracting Plan (Jan 1999)(15 U.S.C. 637(d)(4)(F)(i)).

___ (11) (i) 52.219-23, Notice of Price Evaluation Adjustment for Small Disadvantaged Business Concerns (Sep 2005)(10 U.S.C. 2323) (if the offeror elects to waive the adjustment, it shall so indicate in its offer).

___ (ii) Alternate I (June 2003) of 52.219-23.

___ (12) 52.219-25, Small Disadvantaged Business Participation Program—Disadvantaged Status and Reporting (Oct 1999)(Pub. L. 103-355, section 7102, and 10 U.S.C. 2323).

___ (13) 52.219-26, Small Disadvantaged Business Participation Program—Incentive Subcontracting (Oct 2000)(Pub. L. 103-355, section 7102, and 10 U.S.C. 2323).

___ (14) 52.219-27, Notice of Total Service-Disabled Veteran-Owned Small Business Set-Aside (May 2004) (15 U.S.C. 657 f).

___ (15) 52.219-28, Post Award Small Business Program Rerepresentation (June 2007) (15 U.S.C. 632(a)(2)).

___ (16) 52.222-3, Convict Labor (June 2003)(E.O. 11755).

_X_ (17) 52.222-19, Child Labor—Cooperation with Authorities and Remedies (Feb 2008) (E.O. 13126).

_X_ (18) 52.222-21, Prohibition of Segregated Facilities (Feb 1999).

_X_ (19) 52.222-26, Equal Opportunity (Mar 2007)(E.O. 11246).

_X_ (20) 52.222-35, Equal Opportunity for Special Disabled Veterans, Veterans of the Vietnam Era, and Other Eligible Veterans (Sep 2006)(38 U.S.C. 4212).

_X_ (21) 52.222-36, Affirmative Action for Workers with Disabilities (Jun 1998)(29 U.S.C. 793).

___ (22) 52.222-37, Employment Reports on Special Disabled Veterans, Veterans of the Vietnam Era, and Other Eligible Veterans (Sep 2006)(38 U.S.C. 4212).

___ (23) 52.222-39, Notification of Employee Rights Concerning Payment of Union Dues or Fees (Dec 2004) (E.O. 13201).

___ (24) (i) 52.222-50, Combating Trafficking in Persons (Aug 2007) (Applies to all contracts).

___ (ii) Alternate I (Aug 2007) of 52.222-50.

___ (25) (i) 52.223-9, Estimate of Percentage of Recovered Material Content for EPA-Designated Products (Aug 2000)(42 U.S.C. 6962(c)(3)(A)(ii)).

___ (ii) Alternate I (Aug 2000) of 52.223-9 (42 U.S.C. 6962(i)(2)(C)).

___ (26) 52.223-15, Energy Efficiency in Energy-Consuming Products (Dec 2007) (42 U.S.C. 8259b).

___ (27) (i) 52.223-16, IEEE 1680 Standard for the Environmental Assessment of Personal Computer Products (Dec 2007) (E.O. 13423).

___ (ii) Alternate I (Dec 2007) of 52.223-16.

___ (28) 52.225-1, Buy American Act--Supplies (June 2003)(41 U.S.C. 10a-10d).

_X_ (29) (i) 52.225-3, Buy American Act --Free Trade Agreements – Israeli Trade Act (Aug 2007) (41 U.S.C. 10a-10d, 19 U.S.C. 3301 note, 19 U.S.C. 2112 note, Pub. L. 108-77, 108-78, 108-286, and 109-169).

___ (ii) Alternate I (Jan 2004) of 52.225-3.

___ (iii) Alternate II (Jan 2004) of 52.225-3.

___ (30) 52.225-5, Trade Agreements (Nov 2007) (19 U.S.C. 2501, *et seq.*, 19 U.S.C. 3301 note).

_X_ (31) 52.225-13, Restrictions on Certain Foreign Purchases (Feb 2006) (E.o.s, proclamations, and statutes administered by the Office of Foreign Assets Control of the Department of the Treasury).

___ (32) 52.226-4, Notice of Disaster or Emergency Area Set-Aside (Nov 2007) (42 U.S.C. 5150).

___ (33) 52.226-5, Restrictions on Subcontracting Outside Disaster or Emergency Area (Nov 2007) (42 U.S.C. 5150).

___ (34) 52.232-29, Terms for Financing of Purchases of Commercial Items (Feb 2002) (41 U.S.C. 255(f), 10 U.S.C. 2307(f)).

_X__ (35) 52.232.30, Installment Payments for Commercial Items (Oct 1995)(41 U.S.C. 255(f), 10 U.S.C. 2307(f)).

___ (36) 52.232-33, Payment by Electronic Funds Transfer—Central Contractor Registration (Oct. 2003)(31 U.S.C. 3332).

___ (37) 52.232-34, Payment by Electronic Funds Transfer—Other Than Central Contractor Registration (May 1999)(31 U.S.C. 3332).

___ (38) 52.232-36, Payment by Third Party (May 1999)(31 U.S.C. 3332).

_X__ (39) 52.239-1, Privacy or Security Safeguards (Aug 1996)(5 U.S.C. 552a).

___ (40) (i) 52.247-64, Preference for Privately Owned U.S.-Flag Commercial Vessels (Feb 2006)(46 U.S.C. Appx 1241(b) and 10 U.S.C. 2631).

___ (ii) Alternate I (Apr 2003) of 52.247-64.

(c) The Contractor shall comply with the FAR clauses in this paragraph (c), applicable to commercial services, that the Contracting Officer has indicated as being incorporated in this contract by reference to implement provisions of law or executive orders applicable to acquisitions of commercial items:

[*Contracting Officer check as appropriate.*]

___ (1) 52.222-41, Service Contract Act of 1965 (Nov 2007)(41 U.S.C. 351, *et seq.*).

___ (2) 52.222-42, Statement of Equivalent Rates for Federal Hires (May 1989)(29 U.S.C. 206 and 41 U.S.C. 351, *et seq.*).

___ (3) 52.222-43, Fair Labor Standards Act and Service Contract Act -- Price Adjustment (Multiple Year and Option Contracts) (Nov 2006)(29 U.S.C.206 and 41 U.S.C. 351, *et seq.*).

___ (4) 52.222-44, Fair Labor Standards Act and Service Contract Act -- Price Adjustment (Feb 2002)(29 U.S.C. 206 and 41 U.S.C. 351, *et seq.*).

___ (5) 52.222-51, Exemption from Application of the Service Contract Act to Contracts for Maintenance, Calibration, or Repair of Certain Equipment--Requirements (Nov 2007) (41 U.S.C. 351, et seq.).

___ (6) 52.222-53, Exemption from Application of the Service Contract Act to Contracts for Certain Services--Requirements (Nov 2007) (41 U.S.C. 351, et seq.).

___ (7) 52.237-11, Accepting and Dispensing of $1 Coin (Aug 2007)(31 U.S.C. 5112(p)(1)).

(d) *Comptroller General Examination of Record*. The Contractor shall comply with the provisions of this paragraph (d) if this contract was awarded using other than sealed bid, is in excess of the simplified acquisition threshold, and does not contain the clause at 52.215-2, Audit and Records -- Negotiation.

(1) The Comptroller General of the United States, or an authorized representative of the Comptroller General, shall have access to and right to examine any of the Contractor's directly pertinent records involving transactions related to this contract.

(2) The Contractor shall make available at its offices at all reasonable times the records, materials, and other evidence for examination, audit, or reproduction, until 3 years after final payment under this contract or for any shorter period specified in FAR Subpart 4.7, Contractor Records Retention, of the other clauses of this contract. If this contract is completely or partially terminated, the records relating to the work terminated shall be made available for 3 years after any resulting final termination settlement. Records relating to appeals under the disputes clause or to litigation or the settlement of claims arising under or relating to this contract shall be made available until such appeals, litigation, or claims are finally resolved.

(3) As used in this clause, records include books, documents, accounting procedures and practices, and other data, regardless of type and regardless of form. This does not require the Contractor to create or maintain any record that the Contractor does not maintain in the ordinary course of business or pursuant to a provision of law.

(e)

(1) Notwithstanding the requirements of the clauses in paragraphs (a), (b), (c) and (d) of this clause, the Contractor is not required to flow down any FAR clause, other than those in paragraphs (i) through (vii) of this paragraph in a subcontract for commercial items. Unless otherwise indicated below, the extent of the flow down shall be as required by the clause--

(i) 52.219-8, Utilization of Small Business Concerns (May 2004)(15 U.S.C. 637(d)(2) and (3)), in all subcontracts that offer further subcontracting opportunities. If the subcontract (except subcontracts to small business concerns) exceeds $550,000 ($1,000,000 for construction of any public facility), the subcontractor must include 52.219-8 in lower tier subcontracts that offer subcontracting opportunities.

(ii) 52.222-26, Equal Opportunity (Mar 2007)(E.O. 11246).

(iii) 52.222-35, Equal Opportunity for Special Disabled Veterans, Veterans of the Vietnam Era, and Other Eligible Veterans (Sep 2006)(38 U.S.C. 4212).

(iv) 52.222-36, Affirmative Action for Workers with Disabilities (June 1998)(29 U.S.C. 793).

(v) 52.222-39, Notification of Employee rights Concerning Payment of Union Dues or Fees (Dec 2004) (E.O. 13201).

(vi) 52.222-41, Service Contract Act of 1965, (Nov 2007), flow down required for all subcontracts subject to the Service Contract Act of 1965 (41 U.S.C. 351, *et seq.*)

(vii) 52.222-50, Combating Trafficking in Persons (Aug 2007) (22 U.S.C. 7104(g)). Flow down required in accordance with paragraph (f) of FAR clause 52.222-50.

(viii) 52.222-51, Exemption from Application of the Service Contract Act to Contracts for Maintenance, Calibration, or Repair of Certain Equipment--Requirements (Nov 2007) (41 U.S.C. 351, et seq.)

(ix) 52.222-53, Exemption from Application of the Service Contract Act to Contracts for Certain Services--Requirements (Nov 2007) (41 U.S.C. 351, et seq.)

(x) 52.247-64, Preference for Privately-Owned U.S. Flag Commercial Vessels (Feb 2006) (46 U.S.C. Appx 1241(b) and 10 U.S.C. 2631). Flow down required in accordance with paragraph (d) of FAR clause 52.247-64.

(2) While not required, the contractor may include in its subcontracts for commercial items a minimal number of additional clauses necessary to satisfy its contractual obligations.

(End of Clause)

Alternate I (Feb 2000). As prescribed in 12.301(b)(4), delete paragraph (d) from the basic clause, redesignate paragraph (e) as paragraph (d), and revise the reference to "paragraphs (a), (b), (c), or (d) of this clause" in the redesignated paragraph (d) to read "paragraphs (a), (b), and (c) of this clause".

[Class Deviation- 2001-O0002, Commercial Item Omnibus Clauses for Acquisitions Using the Standard Procurement System. This clause deviation is effective on May 1, 2004, and remains in effect until April 20, 2009, or until other wise rescinded. (2004-o0002)

FAR 52.212-5 CONTRACT TERMS AND CONDITIONS REQUIRED TO IMPLEMENT STATUTES OR EXECUTIVE ORDERS--COMMERCIAL ITEMS (Feb 2008) (DEVIATION)

(a) Comptroller General Examination of Record. The Contractor shall comply with the provisions of this paragraph (a) if this contract was awarded using other than sealed bid, is in excess of the simplified acquisition threshold, and does not contain the clause at 52.215-2, Audit and Records -- Negotiation.

(1) The Comptroller General of the United States, or an authorized representative of the Comptroller General, shall have access to and right to examine any of the Contractor's directly pertinent records involving transactions related to this contract.

(2) The Contractor shall make available at its offices at all reasonable times the records, materials, and other evidence for examination, audit, or reproduction, until 3 years after final payment under this contract or for any shorter period specified in FAR Subpart 4.7, Contractor Records Retention, of the other clauses of this contract. If this contract is completely or partially terminated, the records relating to the work terminated shall be made available for 3 years after any resulting final termination settlement. Records relating to appeals under the disputes clause or to litigation or the settlement of claims arising under or relating to this contract shall be made available until such appeals, litigation, or claims are finally resolved.

(3) As used in this clause, records include books, documents, accounting procedures and practices, and other data, regardless of type and regardless of form. This does not require the Contractor to create or maintain any record that the Contractor does not maintain in the ordinary course of business or pursuant to a provision of law.

(b)

(1) Notwithstanding the requirements of any other clause in this contract, the Contractor is not required to flow down any FAR clause, other than those in paragraphs (i) through (vii) of this paragraph in a subcontract for commercial items. Unless otherwise indicated below, the extent of the flow down shall be as required by the clause.

(i) 52.219-8, Utilization of Small Business Concerns (May 2004)(15 U.S.C. 637(d)(2) and (3)), in all subcontracts that offer further subcontracting opportunities. If the subcontract (except subcontracts to small business concerns) exceeds $550,000 ($1,000,000 for construction of any public facility), the subcontractor must include 52.219-8 in lower tier subcontracts that offer subcontracting opportunities.

(ii) 52.222-26, Equal Opportunity (Mar 2007)(E.O. 11246).

(iii) 52.222-35, Equal Opportunity for Special Disabled Veterans, Veterans of the Vietnam Era, and Other Eligible Veterans (Sep 2006)(38 U.S.C. 4212).

(iv) 52.222-36, Affirmative Action for Workers with Disabilities (June 1998)(29 U.S.C. 793).

(v) 52.222-39, Notification of Employee rights Concerning Payment of Union Dues or Fees (Dec 2004) (E.O. 13201).

(vi) 52.222-41, Service Contract Act of 1965, (Nov 2007), flow down required for all subcontracts subject to the Service Contract Act of 1965 (41 U.S.C. 351, *et seq.*)

(vii) 52.222-50, Combating Trafficking in Persons (Aug 2007) (22 U.S.C. 7104(g)). Flow down required in accordance with paragraph (f) of FAR clause 52.222-50.

(viii) 52.222-51, Exemption from Application of the Service Contract Act to Contracts for Maintenance, Calibration, or Repair of Certain Equipment--Requirements ``(Nov 2007)'' (41 U.S.C. 351, et seq.)
(ix) 52.222-53, Exemption from Application of the Service Contract Act to Contracts for Certain Services--Requirements ``(Nov 2007)'' (41 U.S.C. 351, et seq.)
(x) 52.247-64, Preference for Privately-Owned U.S. Flag Commercial Vessels (Feb 2006) (46 U.S.C. Appx 1241(b) and 10 U.S.C. 2631). Flow down required in accordance with paragraph (d) of FAR clause 52.247-64.

(2) While not required, the contractor may include in its subcontracts for commercial items a minimal number of additional clauses necessary to satisfy its contractual obligations.

(End of Clause)

<u>52.212-1 – Instructions to Offerors – Commercial Items.</u>

As prescribed in 12.301(b)(1), insert the following provision:

Instructions to Offerors – Commercial Items (Nov 2007)

(a) *North American Industry Classification System (NAICS) code and small business size standard.* The NAICS code and small business size standard for this acquisition appear in Block 10 of the solicitation cover sheet (SF 1449). However, the small business size standard for a concern which submits an offer in its own name, but which proposes to furnish an item which it did not itself manufacture, is 500 employees.

(b) *Submission of offers.* Submit signed and dated offers to the office specified in this solicitation at or before the exact time specified in this solicitation. Offers may be submitted on the SF 1449, letterhead stationery, or as otherwise specified in the solicitation. As a minimum, offers must show --

(1) The solicitation number;
(2) The time specified in the solicitation for receipt of offers;
(3) The name, address, and telephone number of the offeror;
(4) A technical description of the items being offered in sufficient detail to evaluate compliance with the requirements in the solicitation. This may include product literature, or other documents, if necessary;
(5) Terms of any express warranty;
(6) Price and any discount terms;
(7) "Remit to" address, if different than mailing address;
(8) A completed copy of the representations and certifications at FAR 52.212-3 (see FAR 52.212-3(l) for those representations and certifications that the offeror shall complete electronically);
(9) Acknowledgment of Solicitation Amendments;
(10) Past performance information, when included as an evaluation factor, to include recent and relevant contracts for the same or similar items and other references (including contract numbers, points of contact with telephone numbers and other relevant information); and
(11) If the offer is not submitted on the SF 1449, include a statement specifying the extent of agreement with all terms, conditions, and provisions included in the solicitation. Offers that fail to furnish required representations or information, or reject the terms and conditions of the solicitation may be excluded from consideration.

(c) *Period for acceptance of offers*. The offeror agrees to hold the prices in its offer firm for 30 calendar days from the date specified for receipt of offers, unless another time period is specified in an addendum to the solicitation.
(d) Product samples. When required by the solicitation, product samples shall be submitted at or prior to the time specified for receipt of offers. Unless otherwise specified in this solicitation, these samples shall be submitted at no expense to the Government, and returned at the sender's request and expense, unless they are destroyed during preaward testing.
(e) Multiple offers. Offerors are encouraged to submit multiple offers presenting alternative terms and conditions or commercial items for satisfying the requirements of this solicitation. Each offer submitted will be evaluated separately.
(f) Late submissions, modifications, revisions, and withdrawals of offers.

(1) Offerors are responsible for submitting offers, and any modifications, revisions, or withdrawals, so as to reach the Government office designated in the solicitation by the time specified in the solicitation. If no time is specified in the solicitation, the time for receipt is 4:30 p.m., local time, for the designated Government office on the date that offers or revisions are due.

(2)

(i) Any offer, modification, revision, or withdrawal of an offer received at the Government office designated in the solicitation after the exact time specified for receipt of offers is "late" and will not be considered unless it is received before award is made, the Contracting Officer determines that accepting the late offer would not unduly delay the acquisition; and—

(A) If it was transmitted through an electronic commerce method authorized by the solicitation, it was received at the initial point of entry to the Government infrastructure not later than 5:00 p.m. one working day prior to the date specified for receipt of offers; or
(B) There is acceptable evidence to establish that it was received at the Government installation designated for receipt of offers and was under the Government's control prior to the time set for receipt of offers; or
(C) If this solicitation is a request for proposals, it was the only proposal received.

(ii) However, a late modification of an otherwise successful offer, that makes its terms more favorable to the Government, will be considered at any time it is received and may be accepted.

(3) Acceptable evidence to establish the time of receipt at the Government installation includes the time/date stamp of that installation on the offer wrapper, other documentary evidence of receipt maintained by the installation, or oral testimony or statements of Government personnel.
(4) If an emergency or unanticipated event interrupts normal Government processes so that offers cannot be received at the Government office designated for receipt of offers by the exact time specified in the solicitation, and urgent Government requirements preclude amendment of the solicitation or other notice of an extension of the closing date, the time specified for receipt of offers will be deemed to be extended to the same time of day specified in the solicitation on the first work day on which normal Government processes resume.
(5) Offers may be withdrawn by written notice received at any time before the exact time set for receipt of offers. Oral offers in response to oral solicitations

may be withdrawn orally. If the solicitation authorizes facsimile offers, offers may be withdrawn via facsimile received at any time before the exact time set for receipt of offers, subject to the conditions specified in the solicitation concerning facsimile offers. An offer may be withdrawn in person by an offeror or its authorized representative if, before the exact time set for receipt of offers, the identity of the person requesting withdrawal is established and the person signs a receipt for the offer.

(g) *Contract award (not applicable to Invitation for Bids).* The Government intends to evaluate offers and award a contract without discussions with offerors. Therefore, the offeror's initial offer should contain the offeror's best terms from a price and technical standpoint. However, the Government reserves the right to conduct discussions if later determined by the Contracting Officer to be necessary. The Government may reject any or all offers if such action is in the public interest; accept other than the lowest offer; and waive informalities and minor irregularities in offers received.

(h) *Multiple awards.* The Government may accept any item or group of items of an offer, unless the offeror qualifies the offer by specific limitations. Unless otherwise provided in the Schedule, offers may not be submitted for quantities less than those specified. The Government reserves the right to make an award on any item for a quantity less than the quantity offered, at the unit prices offered, unless the offeror specifies otherwise in the offer.

(i) *Availability of requirements documents cited in the solicitation.*

(1)(i) The GSA Index of Federal Specifications, Standards and Commercial Item Descriptions, FPMR Part 101-29, and copies of specifications, standards, and commercial item descriptions cited in this solicitation may be obtained for a fee by submitting a request to--

GSA Federal Supply Service Specifications Section
Suite 8100
470 L'Enfant Plaza, SW
Washington, DC 20407
Telephone (202) 619-8925)
Facsimile (202 619-8978).

(ii) If the General Services Administration, Department of Agriculture, or Department of Veterans Affairs issued this solicitation, a single copy of specifications, standards, and commercial item descriptions cited in this solicitation may be obtained free of charge by submitting a request to the addressee in paragraph (i)(1)(i) of this provision. Additional copies will be issued for a fee.

(2) Most unclassified Defense specifications and standards may be downloaded from the following ASSIST websites--

(i) ASSIST (http://assist.daps.dla.mil).

(ii) Quick Search (http://assist.daps.dla.mil/quicksearch/)

(iii) ASSISTdocs.com (http://assistdocs.com).

(3) Documents not available from ASSIST may be ordered from the Department of Defense Single Stock Point (DoDSSP) by—

(i) Using the ASSIST Shopping Wizard (http://assist.daps.dla.mil/wizard);

(ii) Phoning the DoDSSP Customer Service Desk (215) 697-2179, Mon-Fri, 0730 to 1600 EST; or

(iii) Ordering from DoDSSP, Building 4 Section D, 700 Robbins Avenue, Philadelphia, PA 19111-5094, Telephone (215) 697/2197, Facsimile (215) 697-1462.

(4) Nongovernment (voluntary) standards must be obtained from the organization responsible for their preparation, publication, or maintenance.

(j) *Data Universal Numbering System (DUNS) Number.* (Applies to offers exceeding $3,000, and offers of $3,000 or less if the solicitation requires the Contractor to be registered in the Central Contractor Registration (CCR) database. The offeror shall enter, in the block with its name and address on the cover page of its offer, the annotation "DUNS" or "DUNS+4" followed by the DUNS or DUNS+4 number that identifies the offeror's name and address. The DUNS+4 is the DUNS number plus a 4-character suffix that may be assigned at the discretion of the offeror to establish additional CCR records for identifying alternative Electronic Funds Transfer (EFT) accounts (see FAR Subpart 32.11) for the same parent concern. If the offeror does not have a DUNS number, it should contact Dun and Bradstreet directly to obtain one. An offeror within the United States may contact Dun and Bradstreet by calling 1-866-705-5711 or via the Internet at http://www.dnb.com. An offeror located outside the United States must contact the local Dun and Bradstreet office for DUNS number.

(k) *Central Contractor Registration.* Unless exempted by an addendum to this solicitation, by submission of an offer, the offeror acknowledges the requirement that a prospective awardee shall be registered in the CCR database prior to award, during performance and through final payment of any contract resulting from this solicitation. If the Offeror does not become registered in the CCR database in the time prescribed by the Contracting Officer, the Contracting Officer will proceed to award to the next otherwise successful registered Offeror. Offerors may obtain information on registration and annual confirmation requirements via the Internet at http://www.ccr.gov or by calling 1-888-227-2423 or 269-961-5757.

(l) *Debriefing.* If a post-award debriefing is given to requesting offerors, the Government shall disclose the following information, if applicable:

(1) The agency's evaluation of the significant weak or deficient factors in the debriefed offeror's offer.

(2) The overall evaluated cost or price and technical rating of the successful and debriefed offeror and past performance information on the debriefed offeror.

(3) The overall ranking of all offerors, when any ranking was developed by the agency during source selection.

(4) A summary of rationale for award;

(5) For acquisitions of commercial items, the make and model of the item to be delivered by the successful offeror.

(6) Reasonable responses to relevant questions posed by the debriefed offeror as to whether source-selection procedures set forth in the solicitation, applicable regulations, and other applicable authorities were followed by the agency.

(End of Provision)

52.212-3 – Offeror Representations and Certifications – Commercial Items (Nov 2007)

An offeror shall complete only paragraph (l) of this provision if the offeror has completed the annual representations and certificates electronically at http://orca.bpn.gov . If an offeror has not completed the annual representations and certifications electronically at the ORCA website, the offeror shall complete only paragraphs (b) through (k) of this provision.

(a) *Definitions.* As used in this provision--

"Emerging small business" means a small business concern whose size is no greater than 50 percent of the numerical size standard for the NAICS code designated.

"Forced or indentured child labor" means all work or service—

(1) Exacted from any person under the age of 18 under the menace of any penalty for its nonperformance and for which the worker does not offer himself voluntarily; or

(2) Performed by any person under the age of 18 pursuant to a contract the enforcement of which can be accomplished by process or penalties.

"Manufactured end product" means any end product in Federal Supply Classes (FSC) 1000-9999, except—

(1) FSC 5510, Lumber and Related Basic Wood Materials;
(2) Federal Supply Group (FSG) 87, Agricultural Supplies;
(3) FSG 88, Live Animals;
(4) FSG 89, Food and Related Consumables;
(5) FSC 9410, Crude Grades of Plant Materials;
(6) FSC 9430, Miscellaneous Crude Animal Products, Inedible;
(7) FSC 9440, Miscellaneous Crude Agricultural and Forestry Products;
(8) FSC 9610, Ores;
(9) FSC 9620, Minerals, Natural and Synthetic; and
(10) FSC 9630, Additive Metal Materials.

"Place of manufacture" means the place where an end product is assembled out of components, or otherwise made or processed from raw materials into the finished product that is to be provided to the Government. If a product is disassembled and reassembled, the place of reassembly is not the place of manufacture.

"Service-disabled veteran-owned small business concern"—

(1) Means a small business concern—

(i) Not less than 51 percent of which is owned by one or more service-disabled veterans or, in the case of any publicly owned business, not less than 51 percent of the stock of which is owned by one or more service-disabled veterans; and

(ii) The management and daily business operations of which are controlled by one or more service-disabled veterans or, in the case of a service-disabled veteran with permanent and severe disability, the spouse or permanent caregiver of such veteran.

(2) Service-disabled veteran means a veteran, as defined in 38 U.S.C. 101(2), with a disability that is service-connected, as defined in 38 U.S.C. 101(16).

"Small business concern" means a concern, including its affiliates, that is independently owned and operated, not dominant in the field of operation in which it is bidding on Government contracts, and qualified as a small business under the criteria in 13 CFR Part 121 and size standards in this solicitation.

"Veteran-owned small business concern" means a small business concern—

(1) Not less than 51 percent of which is owned by one or more veterans(as defined at 38 U.S.C. 101(2)) or, in the case of any publicly owned business, not less than 51 percent of the stock of which is owned by one or more veterans; and

(2) The management and daily business operations of which are controlled by one or more veterans.

"Women-owned business concern" means a concern which is at least 51 percent owned by one or more women; or in the case of any publicly owned business, at least 51 percent of the its stock is owned by one or more women; and whose management and daily business operations are controlled by one or more women.

"Women-owned small business concern" means a small business concern --

(1) That is at least 51 percent owned by one or more women or, in the case of any publicly owned business, at least 51 percent of the stock of which is owned by one or more women; and

(2) Whose management and daily business operations are controlled by one or more women.

(b) *Taxpayer identification number (TIN) (26 U.S.C. 6109, 31 U.S.C. 7701).* (Not applicable if the offeror is required to provide this information to a central contractor registration database to be eligible for award.)

(1) All offerors must submit the information required in paragraphs (b)(3) through (b)(5) of this provision to comply with debt collection requirements of 31 U.S.C. 7701(c) and 3325(d), reporting requirements of 26 U.S.C. 6041, 6041A, and 6050M, and implementing regulations issued by the Internal Revenue Service (IRS).

(2) The TIN may be used by the government to collect and report on any delinquent amounts arising out of the offeror's relationship with the Government (31 U.S.C. 7701(c)(3)). If the resulting contract is subject to the payment reporting requirements described in FAR 4.904, the TIN provided hereunder may be matched with IRS records to verify the accuracy of the offeror's TIN.]

(3) Taxpayer Identification Number (TIN).

* TIN:______________________.

* TIN has been applied for.

* TIN is not required because:

* Offeror is a nonresident alien, foreign corporation, or foreign partnership that does not have income effectively connected with the conduct of a trade or business in the United States and does not have an office or place of business or a fiscal paying agent in the United States;

* Offeror is an agency or instrumentality of a foreign government;

* Offeror is an agency or instrumentality of the Federal Government;

(4) Type of organization.

* Sole proprietorship;

* Partnership;

* Corporate entity (not tax-exempt);

* Corporate entity (tax-exempt);
* Government entity (Federal, State, or local);
* Foreign government;
* International organization per 26 CFR 1.6049-4;
* Other ____________________.
(5) Common parent.
* Offeror is not owned or controlled by a common parent:
* Name and TIN of common parent:
Name ____
TIN ____

(c) Offerors must complete the following representations when the resulting contract is to be performed in the United States or its outlying areas. Check all that apply.

(1) *Small business concern.* The offeror represents as part of its offer that it ~~* is,~~ * is not a small business concern.

(2) Veteran-owned small business concern. [Complete only if the offeror represented itself as a small business concern in paragraph (c)(1) of this provision.] The offeror represents as part of its offer that it * is, * is not a veteran-owned small business concern.

(3) Service-disabled veteran-owned small business concern. [Complete only if the offeror represented itself as a veteran-owned small business concern in paragraph (c)(2) of this provision.] The offeror represents as part of its offer that it * is, * is not a service-disabled veteran-owned small business concern.

(4) Small disadvantaged business concern. [Complete only if the offeror represented itself as a small business concern in paragraph (c)(1) of this provision.] The offeror represents, for general statistical purposes, that it * is, * is not, a small disadvantaged business concern as defined in 13 CFR 124.1002.

(5) Women-owned small business concern. [Complete only if the offeror represented itself as a small business concern in paragraph (c)(1) of this provision.] The offeror represents that it * is, * is not a women-owned small business concern.

Note: Complete paragraphs (c)(6) and (c)(7) only if this solicitation is expected to exceed the simplified acquisition threshold.

(6) Women-owned business concern (other than small business concern). [Complete only if the offeror is a women-owned business concern and did not represent itself as a small business concern in paragraph (c)(1) of this provision.]. The offeror represents that it * is, a women-owned business concern.

(7) *Tie bid priority for labor surplus area concerns.* If this is an invitation for bid, small business offerors may identify the labor surplus areas in which costs to be incurred on account of manufacturing or production (by offeror or first-tier subcontractors) amount to more than 50 percent of the contract price:

____

(8) Small Business Size for the Small Business Competitiveness Demonstration Program and for the Targeted Industry Categories under the Small Business Competitiveness Demonstration Program. *[Complete only if the offeror has represented itself to be a small business concern under the size standards for this solicitation.]*

(i) [*Complete only for solicitations indicated in an addendum as being set-aside for emerging small businesses in one of the designated industry* *groups (DIGs).*] The offeror represents as part of its offer that it * is, * is not an emerging small business.

(ii) [*Complete only for solicitations indicated in an addendum as being for one of the targeted industry categories (TICs) or designated industry groups (DIGs).*] Offeror represents as follows:

(A) Offeror's number of employees for the past 12 months (check the Employees column if size standard stated in the solicitation is expressed in terms of number of employees); or

(B) Offeror's average annual gross revenue for the last 3 fiscal years (check the Average Annual Gross Number of Revenues column if size standard stated in the solicitation is expressed in terms of annual receipts).

(Check one of the following):

Number of Employees	**Average Annual Gross Revenues**
50 or fewer	$1 million or less
51-100	$1,000,001-$2 million
101-250	$2,000,001-$3.5 million
251-500	$3,500,001-$5 million
501-750	$5,000,001-$10 million
751-1,000	$10,000,001-$17 million
Over 1,000	Over $17 million

(9) [Complete only if the solicitation contains the clause at FAR 52.219-23, Notice of Price Evaluation Adjustment for Small Disadvantaged Business Concerns, or FAR 52.219-25, Small Disadvantaged Business Participation Program—Disadvantaged Status and Reporting, and the offeror desires a benefit based on its disadvantaged status.]

(i) *General.* The offeror represents that either—

(A) It * is, * is not certified by the Small Business Administration as a small disadvantaged business concern and identified, on the date of this representation, as a certified small disadvantaged business concern in the database maintained by the Small Business Administration (PRO-Net), and that no material change in disadvantaged ownership and control has occurred since its certification, and, where the concern is owned by one or more individuals claiming disadvantaged status, the net worth of each individual upon whom the certification is based does not exceed $750,000 after taking into account the applicable exclusions set forth at 13 CFR 124.104(c)(2); or

(B) It *has, * has not submitted a completed application to the Small Business Administration or a Private Certifier to be certified as a small disadvantaged business concern in accordance with 13 CFR 124, Subpart B, and a decision on that application is pending, and that no material change in disadvantaged ownership and control has occurred since its application was submitted.

(ii) *Joint Ventures under the Price Evaluation Adjustment for Small Disadvantaged Business Concerns.* The offeror represents, as part of its offer, that it is a joint venture that complies with the requirements in 13 CFR 124.1002(f) and that the representation in paragraph (c)(9)(i) of this provision is accurate for the small disadvantaged business concern that is participating in the joint venture. [*The offeror shall enter the name of the small disadvantaged business concern that is participating in the joint venture:* ______________.]

(10) HUBZone small business concern. [Complete only if the offeror represented itself as a small business concern in paragraph (c)(1) of this provision.] The offeror represents, as part of its offer, that--

(i) It * is, * is not a HUBZone small business concern listed, on the date of this representation, on the List of Qualified HUBZone Small Business Concerns maintained by the Small Business Administration, and no material change in ownership and control, principal office, or HUBZone employee percentage has occurred since it was certified by the Small Business Administration in accordance with 13 CFR part 126; and

(ii) It * is, * not a joint venture that complies with the requirements of 13 CFR part 126, and the representation in paragraph (c)(10)(i) of this provision is accurate for the HUBZone small business concern or concerns that are participating in the joint venture. [*The offeror shall enter the name or names of the HUBZone small business concern or concerns that are participating in the joint venture*: __________.] Each HUBZone small business concern participating in the joint venture shall submit a separate signed copy of the HUBZone representation.

(d) *Representations required to implement provisions of Executive Order 11246* --

(1) Previous contracts and compliance. The offeror represents that --

(i) It ~~*has,~~ * has not, participated in a previous contract or subcontract subject to the Equal Opportunity clause of this solicitation; and

(ii) It ~~*has,~~ * has not, filed all required compliance reports.

(2) *Affirmative Action Compliance.* The offeror represents that --

(i) It ~~*has developed and has on file,~~ * has not developed and does not have on file, at each establishment, affirmative action programs required by rules and regulations of the Secretary of Labor (41 CFR parts 60-1 and 60-2), or

(ii) It * has not previously had contracts subject to the written affirmative action programs requirement of the rules and regulations of the Secretary of Labor.

(e) *Certification Regarding Payments to Influence Federal Transactions* (31 U.S.C. 1352). (Applies only if the contract is expected to exceed $100,000.) By submission of its offer, the offeror certifies to the best of its knowledge and belief that no Federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress or an employee of a Member of Congress on his or her behalf in connection with the award of any resultant contract. If any registrants under the Lobbying Disclosure Act of 1995 have made a lobbying contact on behalf of the offeror with respect to this contract, the offeror shall complete and submit, with its offer, OMB Standard Form LLL, Disclosure of Lobbying Activities, to provide the name of the registrants. The offeror need not report regularly employed officers or employees of the offeror to whom payments of reasonable compensation were made.

(f) *Buy American Act Certificate.* (Applies only if the clause at Federal Acquisition Regulation (FAR) 52.225-1, Buy American Act – Supplies, is included in this solicitation.)

(1) The offeror certifies that each end product, except those listed in paragraph (f)(2) of this provision, is a domestic end product and that the offeror has considered components of unknown origin to have been mined, produced, or manufactured outside the United States. The offeror shall list as foreign end products those end products manufactured in the United States that do not qualify as domestic end products. The terms "component," "domestic end product," "end product," "foreign end product," and "United States" are defined in the clause of this solicitation entitled "Buy American Act—Supplies."

(2) Foreign End Products:

LINE ITEM NO.	COUNTRY OF ORIGIN

[List as necessary]

(3) The Government will evaluate offers in accordance with the policies and procedures of FAR Part 25.

(g)

(1) *Buy American Act -- Free Trade Agreements -- Israeli Trade Act Certificate.* (Applies only if the clause at FAR 52.225-3, Buy American Act -- Free Trade Agreements -- Israeli Trade Act, is included in this solicitation.)

(i) The offeror certifies that each end product, except those listed in paragraph (g)(1)(ii) or (g)(1)(iii) of this provision, is a domestic end product and that the offeror has considered components of unknown origin to have been mined, produced, or manufactured outside the United States. The terms "Bahrainian or Moroccan end product," "component," "domestic end product," "end product," "foreign end product," "Free Trade Agreement country," "Free Trade Agreement country end product," "Israeli end product," and 'United States' are defined in the clause of this solicitation entitled "Buy American Act--Free Trade Agreements--Israeli Trade Act."

(ii) The offeror certifies that the following supplies are Free Trade Agreement country end products (other than Bahrainian or Moroccan end products) or Israeli end products as defined in the clause of this solicitation entitled "Buy American Act—Free Trade Agreements—Israeli Trade Act":

Free Trade Agreement Country End Products (Other than Bahrainian or Moroccan End Products) or Israeli End Products:

LINE ITEM NO.	COUNTRY OF ORIGIN

[List as necessary]

(iii) The offeror shall list those supplies that are foreign end products (other than those listed in paragraph (g)(1)(ii) or this provision) as defined in the clause of this solicitation entitled "Buy American Act—Free Trade Agreements—Israeli Trade Act." The offeror shall list as other foreign end products those end products manufactured in the United States that do not qualify as domestic end products.

Other Foreign End Products:

LINE ITEM NO.	COUNTRY OF ORIGIN

[List as necessary]

(iv) The Government will evaluate offers in accordance with the policies and procedures of FAR Part 25.

(2) *Buy American Act—Free Trade Agreements—Israeli Trade Act Certificate, Alternate I.* If Alternate I to the clause at FAR 52.225-3 is included in this solicitation, substitute the following paragraph (g)(1)(ii) for paragraph (g)(1)(ii) of the basic provision:

(g)(1)(ii) The offeror certifies that the following supplies are Canadian end products as defined in the clause of this solicitation entitled "Buy American Act—Free Trade Agreements—Israeli Trade Act":

Canadian End Products:

Line Item No.:

____

[List as necessary]

(3) *Buy American Act—Free Trade Agreements—Israeli Trade Act Certificate, Alternate II.* If Alternate II to the clause at FAR 52.225-3 is included in this solicitation, substitute the following paragraph (g)(1)(ii) for paragraph (g)(1)(ii) of the basic provision:

(g)(1)(ii) The offeror certifies that the following supplies are Canadian end products or Israeli end products as defined in the clause of this solicitation entitled "Buy American Act--Free Trade Agreements--Israeli Trade Act":

Canadian or Israeli End Products:

Line Item No.:	Country of Origin:

[*List as necessary*]

(4) *Trade Agreements Certificate*. (Applies only if the clause at FAR 52.225-5, Trade Agreements, is included in this solicitation.)

(i) The offeror certifies that each end product, except those listed in paragraph (g)(4)(ii) of this provision, is a U.S.-made or designated country end product as defined in the clause of this solicitation entitled "Trade Agreements."

(ii) The offeror shall list as other end products those end products that are not U.S.-made or designated country end products.

Other End Products

Line Item No.:	Country of Origin:

[*List as necessary*]

(iii) The Government will evaluate offers in accordance with the policies and procedures of FAR Part 25. For line items covered by the WTO GPA, the Government will evaluate offers of U.S.-made or designated country end products without regard to the restrictions of the Buy American Act. The Government will consider for award only offers of U.S.-made or designated country end products unless the Contracting Officer determines that there are no offers for such products or that the offers for such products are insufficient to fulfill the requirements of the solicitation.

(h) *Certification Regarding Debarment, Suspension or Ineligibility for Award (Executive Order 12689)*. (Applies only if the contract value is expected to exceed the simplified acquisition threshold.) The offeror certifies, to the best of its knowledge and belief, that the offeror and/or any of its principals--

(1) *~~Are~~, * are not presently debarred, suspended, proposed for debarment, or declared ineligible for the award of contracts by any Federal agency; and

(2) *~~Have~~, * have not, within a three-year period preceding this offer, been convicted of or had a civil judgment rendered against them for: commission of fraud or a criminal offense in connection with obtaining, attempting to obtain, or performing a Federal, state or local government contract or subcontract; violation of Federal or state antitrust statutes relating to the submission of offers; or commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, tax evasion, or receiving stolen property; and

(3) *~~Are~~, * are not presently indicted for, or otherwise criminally or civilly charged by a Government entity with, commission of any of these offenses.

(i) *Certification Regarding Knowledge of Child Labor for Listed End Products (Executive Order 13126). [The Contracting Officer must list in paragraph (i)(1) any end products being acquired under this solicitation that are included in the List of Products Requiring Contractor Certification as to Forced or Indentured Child Labor, unless excluded at 22.1503(b).]*

(1) Listed End Product

Listed End Product:	Listed Countries of Origin:

(2) Certification. [If the Contracting Officer has identified end products and countries of origin in paragraph (i)(1) of this provision, then the offeror must certify to either (i)(2)(i) or (i)(2)(ii) by checking the appropriate block.]

[ ] (i) The offeror will not supply any end product listed in paragraph (i)(1) of this provision that was mined, produced, or manufactured in the corresponding country as listed for that product.

[ ] (ii) The offeror may supply an end product listed in paragraph (i)(1) of this provision that was mined, produced, or manufactured in the corresponding country as listed for that product. The offeror certifies that is has made a good faith effort to determine whether forced or indentured child labor was used to mine, produce, or manufacture any such end product furnished under this contract. On the basis of those efforts, the offeror certifies that it is not aware of any such use of child labor.

(j) *Place of manufacture.* (Does not apply unless the solicitation is predominantly for the acquisition of manufactured end products.) For statistical purposes only, the offeror shall indicate whether the place of manufacture of the end products it expects to provide in response to this solicitation is predominantly—

(1) [x] In the United States (Check this box if the total anticipated price of offered end products manufactured in the United States exceeds the total anticipated price of offered end products manufactured outside the United States); or

(2) [ ] Outside the United States.

(k) Certificates regarding exemptions from the application of the Service Contract Act. (Certification by the offeror as to its compliance with respect to the contract also constitutes its certification as to compliance by its subcontractor if it subcontracts out the exempt services.) [The contracting officer is to check a box to indicate if paragraph (k)(1) or (k)(2) applies.]

(1) [ ] Maintenance, calibration, or repair of certain equipment as described in FAR 22.1003-4(c)(1). The offeror [ ] does [ ] does not certify that—

(i) The items of equipment to be serviced under this contract are used regularly for other than Governmental purposes and are sold or traded by the offeror in substantial quantities to the general public in the course of normal business operations;

(ii) The services will be furnished at prices which are, or are based on, established catalog or market prices (see FAR 22.1003-4(c)(2)(ii)) for the maintenance, calibration, or repair of such equipment; and

(iii) The compensation (wage and fringe benefits) plan for all service employees performing work under the contract will be the same as that used for these employees and equivalent employees servicing the same equipment of commercial customers.

(2) [ ] Certain services as described in FAR 22.1003-4(d)(1). The offeror [ ] does [ ] does not certify that—

(i) The services under the contract are offered and sold regularly to non-Governmental customers, and are provided by the offeror (or subcontractor in the case of an exempt subcontract) to the general public in substantial quantities in the course of normal business operations;
(ii) The contract services will be furnished at prices that are, or are based on, established catalog or market prices (see FAR 22.1003-4(d)(2)(iii));
(iii) Each service employee who will perform the services under the contract will spend only a small portion of his or her time (a monthly average of less than 20 percent of the available hours on an annualized basis, or less than 20 percent of available hours during the contract period if the contract period is less than a month) servicing the Government contract; and
(iv) The compensation (wage and fringe benefits) plan for all service employees performing work under the contract is the same as that used for these employees and equivalent employees servicing commercial customers.

(3) If paragraph (k)(1) or (k)(2) of this clause applies—

(i) If the offeror does not certify to the conditions in paragraph (k)(1) or (k)(2) and the Contracting Officer did not attach a Service Contract Act wage determination to the solicitation, the offeror shall notify the Contracting Officer as soon as possible; and
(ii) The Contracting Officer may not make an award to the offeror if the offeror fails to execute the certification in paragraph (k)(1) or (k)(2) of this clause or to contact the Contracting Officer as required in paragraph (k)(3)(i) of this clause.

(l)

(1) *Annual Representations and Certifications.* Any changes provided by the offeror in paragraph (l)(2) of this provision do not automatically change the representations and certifications posted on the Online Representations and Certifications Application (ORCA) website.

(2) The offeror has completed the annual representations and certifications electronically via the ORCA website at http://orca.bpn.gov .After reviewing the ORCA database information, the offeror verifies by submission of this offer that the representation and certifications currently posted electronically at FAR 52.212-3, Offeror Representations and certifications—Commercial Items, have been entered or updated in the last 12 months, are current, accurate, complete, and applicable to this solicitation (including the business size standard applicable to the NAICS code referenced for this solicitation), as of the date of this offer and are incorporated in this offer by reference (see FAR 4.1201), except for paragraphs ____________. *[Offeror to identify the applicable paragraphs at (b) through (k) of this provision that the offeror has completed for the purposes of this solicitation only, if any. These amended representation(s) and/or certification(s) are also incorporated in this offer and are current, accurate, and complete as of the date of this offer. Any changes provided by the offeror are*

applicable to this solicitation only, and do not result in an update to the representations and certifications posted on ORCA.]

(End of Provision)

Alternate I (Apr 2002). As prescribed in 12.301(b)(2), add the following paragraph (c)(11) to the basic provision:

(11) (Complete if the offeror has represented itself as disadvantaged in paragraph (c)(4) or (c)(9) of this provision.) [*The offeror shall check the category in which its ownership falls*]:

____ Black American.

___ Hispanic American.

___ Native American (American Indians, Eskimos, Aleuts, or Native Hawaiians).

___ Asian-Pacific American (persons with origins from Burma, Thailand, Malaysia, Indonesia, Singapore, Brunei, Japan, China, Taiwan, Laos, Cambodia (Kampuchea), Vietnam, Korea, The Philippines, U.S. Trust Territory or the Pacific Islands (Republic of Palau), Republic of the Marshall Islands, Federated States of Micronesia, the Commonwealth of the Northern Mariana Islands, Guam, Samoa, Macao, Hong Kong, Fiji, Tonga, Kiribati, Tuvalu, or Nauru).

___ Subcontinent Asian (Asian-Indian) American (persons with origins from India, Pakistan, Bangladesh, Sri Lanka, Bhutan, the Maldives Islands, or Nepal).

___ Individual/concern, other than one of the preceding.

Alternate II (Oct 2000). As prescribed in 12.301(b)(2), add the following paragraph (c)(9)(iii) to the basic provision:

(iii) Address. The offeror represents that its address __ is, x is not in a region for which a small disadvantaged business procurement mechanism is authorized and its address has not changed since its certification as a small disadvantaged business concern or submission of its application for certification. The list of authorized small disadvantaged business procurement mechanisms and regions is posted at http://www.arnet.gov/References/sdbadjustments.htm. The offeror shall use the list in effect on the date of this solicitation. "Address," as used in this provision, means the address of the offeror as listed on the Small Business Administration's register of small disadvantaged business concerns or the address on the completed application that the concern has submitted to the Small Business Administration or a Private Certifier in accordance with 13 CFR part 124, subpart B. For joint ventures, "address" refers to the address of the small disadvantaged business concern that is participating in the joint venture.

(b) (6)

(b) (6)

http://www.peacefire.org

AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT

1. CONTRACT ID CODE

2. AMENDMENT/MODIFICATION NO. 001	3. EFFECTIVE DATE 09/17/2012	4. REQUISITION/PURCHASE REQ. NO. See Lines	5. PROJECT NO. (If applicable)

6. ISSUED BY CODE CON

Broadcasting Board of Governors
Office Of Contracts
330 C Street SW
Room 4300
Washington, DC 20237

7. ADMINISTERED BY (If other than Item 6) CODE

8. NAME AND ADDRESS OF CONTRACTOR (No., street, country, state and ZIP Code)

TOR SOLUTIONS CORPORATION
969 MAIN STREET, SUITE 206
WALPOLE, MA 02081-2972

CODE D11091700 FACILITY CODE 001

(X)

9A. AMENDMENT OF SOLICITATION NO.

9B. DATED (SEE ITEM 11)

X 10A. MODIFICATION OF CONTRACT/ORDER NO.
BBG50-J-12-0508

10B. DATED (SEE ITEM 11)
06/18/2012

11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS

□ The above numbered solicitation is amended as set forth in Item 14. The hour and date specified for receipt of Offers □ is extended, □ is not extended,

Offers must acknowledge receipt of this amendment prior to the hour and date specified in the solicitation or as amended, by one of the following methods: (a) By completing Items 8 and 15, and returning _______________ copies of the amendment; (b) By acknowledging receipt of this amendment on each copy of the offer submitted; or (c) By separate letter or telegram which includes a reference to the solicitation and amendment numbers. FAILURE OF YOUR ACKNOWLEDGMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATE SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER. If by virtue of this amendment your desire to change an offer already submitted, such change may be made by telegram or letter, provided each telegram or letter makes reference to the solicitation and this amendment, and is received prior to the opening hour and date specified.

12. ACCOUNTING AND APPROPRIATION DATA (If required)
See Line Item Detail

13. THIS ITEM ONLY APPLIES TO MODIFICATION OF CONTRACTS/ORDERS. IT MODIFIES THE CONTRACT/ORDER NO. AS DESCRIBED IN ITEM 14.

CHECK ONE	
	A. THIS CHANGE ORDER IS ISSUED PURSUANT TO: (Specify authority) THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT ORDER NO. IN ITEM 10A.
X	B. THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES (such as changes in paying office, appropriation date, etc.) SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103(b).
	C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF:
	D. OTHER (Specify type of modification and authority)

E. IMPORTANT: Contractor ☒ is not, □ is required to sign this document and return copies to the issuing office.

14. DESCRIPTION OF AMENDMENT/MODIFICATION (Organized by UCF section headings, including solicitation/contract subject matter where feasible.)
BBG50-J-12-0508 IS MODIFIED TO EXERCISE OPTIONS C.2.10; C2.12; C.213 AND C.2.14

Except as provided herein, all terms and conditions of the document referenced in Item 9A or 10A, as heretofore changed, remains unchanged and in full force and effect.

15A. NAME AND TITLE OF SIGNER (Type or print)		16A. NAME AND TITLE OF CONTRACTING OFFICER (Type or print) Gary Hosford	
15B. CONTRACTOR/OFFEROR ________________________ (Signature of person authorized to sign)	15C. DATE SIGNED	16B. UNITED STATES OF AMERICA By [redacted] (b) (6) (Signature of Contracting Officer)	16C. DATE SIGNED 09/17/2012

NSN 7540-01-152-8070
Previous edition unusable

STANDARD FORM 30 (REV. 10-83)
Prescribed by GSA FAR (48 CFR) 53.243

Table of Contents

Summary Info Continuation Page
Continuation Sheet

Number	Quantity	Unit of Issue	Unit Price	Total Cost (Incl. disc and tax)
1	Original : 12.000000		Original: $25,000.0000	Original:$300,000.00
	Change: 0.000000		Change: $0.0000	Change: $0.00
	Total : 12.000000	EA	Total: $25,000.0000	Total: $300,000.00

Period of Performance: 06/18/2012 - 06/17/2013
Description: This is an IDIQ {Referencing BBG50-D-11-0061} for Task 5 for the Peer-to-Peer with TOR. (SEE STATEMENT OF WORK)

Extended Description:

Delivery Schedule:

Delivery Number	Delivery Date	Quantity

Purchase Request Reference Line:T013-12-IQ-00038 - 0

Contract/BPA Number:BBG50-D-11-0061 - 1

1.
2012-0206-TSI-T013-4335-2544-250200
Original Total: $300,000.00
Change Total: $0.00
Total: $300,000.00

Number	Quantity	Unit of Issue	Unit Price	Total Cost (Incl. disc and tax)
2	Original : 12.000000		Original: $39,633.3500	Original:$475,600.20
	Change: 0.000000		Change: $0.0000	Change: $0.00
	Total : 12.000000	YR	Total: $39,633.3500	Total: $475,600.20

Period of Performance: 06/18/2012 - 06/17/2013
Description: This is a requisition for TOR expansion Task #5 under the IDIQ. BBG50-D-11-61 See Attached for SOW

Extended Description:

Delivery Schedule:

Delivery Number	Delivery Date	Quantity

Purchase Request Reference Line:E013-12-IQ-00005 - 0

Contract/BPA Number:BBG50-D-11-0061 - 1

1.
2011-2012-0206-ENG-E013-4335-2544-454000-2011
Original Total: $475,600.20
Change Total: $0.00
Total: $475,600.20

Number	Quantity	Unit of Issue	Unit Price	Total Cost (Inc. disc and tax)
3	Original :		Original: $0.0000	Original:$0.00
	Change: 1.000000		Change: $126,000.0000	Change: $126,000.00
	Total : 1.000000	EA	Total: $126,000.0000	Total: $126,000.00

Period of Performance: 09/18/2012 - 09/17/2013
Description: This is Referencing: BBG50-J-12-0508 Exercise Option on Task Order # 5.

Extended Description: C.2.10 - Improvements to allow TOR relays to operate on dynamic IP addresses.

Delivery Schedule:

Delivery Number	Delivery Date	Quantity

Purchase Request Reference Line:T013-12-IQ-00096 - 0

Contract/BPA Number:BBG50-D-11-0061 - 1

1.
2012-0206-TSI-T013-4335-2544-250200
Original Total: $0.00
Change Total: $126,000.00
Total: $126,000.00

Number	Quantity	Unit of Issue	Unit Price	Total Cost (Inc. disc and tax)
4	Original :		Original: $0.0000	Original:$0.00
	Change: 1.000000		Change: $100,800.0000	Change: $100,800.00
	Total : 1.000000	EA	Total: $100,800.0000	Total: $100,800.00

Period of Performance: 09/18/2012 - 09/17/2013
Description: C.2.12 - Improvements to TOR button to improve security & media streaming.

Extended Description: C.2.10 - Improvements to allow TOR relays to operate on dynamic IP addresses.

Delivery Schedule:

Delivery Number	Delivery Date	Quantity

Purchase Request Reference Line:T013-12-IQ-00096 - 0

Contract/BPA Number:BBG50-D-11-0061 - 2

1.
2012-0206-TSI-T013-4335-2544-250200
Original Total: $0.00
Change Total: $100,800.00
Total: $100,800.00

Number	Quantity	Unit of Issue	Unit Price	Total Cost (Inc. disc and tax)
5	Original :		Original: $0.0000	Original:$0.00
	Change: 1.000000		Change: $189,000.0000	Change: $189,000.00
	Total : 1.000000	EA	Total: $189,000.0000	Total: $189,000.00

Period of Performance: 09/18/2012 - 09/17/2013
Description: C.2.13 - Improvements for safe use of Flash within TOR.

Extended Description: C.2.10 - Improvements to allow TOR relays to operate on dynamic IP addresses.

Delivery Schedule:

Delivery Number	**Delivery Date**	**Quantity**

Purchase Request Reference Line:T013-12-IQ-00096 - 0

Contract/BPA Number:BBG50-D-11-0061 - 3

1.
2012-0206-TSI-T013-4335-2544-250200
Original Total: $0.00
Change Total: $189,000.00
Total: $189,000.00

Number	Quantity	Unit of Issue	Unit Price	Total Cost (inc. disc and tax)
6	Original : Change: 1.000000 Total : 1.000000	EA	Original: $0.0000 Change: $50,000.0000 Total: $50,000.0000	Original:$0.00 Change: $50,000.00 Total: $50,000.00

Period of Performance: 09/18/2012 - 09/17/2013
Description: C.2.14 - Improvements to HTTPS Everywhere extension.

Extended Description: Suggested Vendor: TOR Solutions Corporation 969 Main Street, suite 206 Walpole, MA 02081-2972

Delivery Schedule:

Delivery Number	**Delivery Date**	**Quantity**

Purchase Request Reference Line:T013-12-IQ-00096 - 0

Contract/BPA Number:BBG50-D-11-0061 - 4

1.
2012-0206-TSI-T013-4335-2544-250200
Original Total: $0.00
Change Total: $50,000.00
Total: $50,000.00

Accounting Line Accounting and Appropriations Data:

Accounting and Funding Total:

Previous Total: $775,600.20
Modification Total: $465,800.00
Grand Total: $1,241,400.20

IDC Constraints Line Item

Line Number	Minumum Quantity	Minimum Amount	Maximum Quantity	Maximum Amount
1	0.000000	$0.00	0.000000	$0.00
2	0.000000	$0.00	0.000000	$0.00
3	0.000000	$0.00	0.000000	$0.00
4	0.000000	$0.00	0.000000	$0.00
5	0.000000	$0.00	0.000000	$0.00

Line Number	Minumum Quantity	Minimum Amount	Maximum Quantity	Maximum Amount
6	0.000000	$0.00	0.000000	$0.00

Descriptions & Specifications
IDC Constraints Document

1000 STATEMENT OF WORK

SECTION C

DESCRIPTION/SPECIFICATIONS/STATEMENT OF WORK

C.1 BACKGROUND

The Broadcasting Board of Governors (BBG) oversees the mission and operation of several overseas broadcasting entities of the United States Government (USG). The International Broadcasting Bureau (IBB) oversees the daily operations of several USG broadcasters, including the Voice of America (VOA), and is responsible for all contractual and fiscal matters pertaining to broadcast operations. The IBB's Internet anti-censorship program seeks to ensure Internet users in target countries are able to access USG broadcasters' web sites to access their news and other programming, using a variety of tools to counter foreign government-sponsored Internet censorship controls.

This Statement of Work defines those duties the Contractor shall perform to enable the IBB to meet its goals of using Tor as a tool to further its Internet anti-censorship efforts. Tor is open source software, Tor and related software source code and binaries are available as free downloads from https://www.torproject.org/projects/projects.html.en and the source code can be freely modified to meet the requirements of this SOW (per the license terms contained on the project pages on the Tor Project web site).

C.2 TECHNICAL REQUIREMENTS

C.2.1 The Contractor shall provide and operate, either directly or by subcontracting, 125 Tor relay servers, using leased cloud virtual servers or dedicated hosting services, with a total aggregate bandwidth (burst capacity) of no less than 12.5 Gigabits-per-second (Gbps) and monthly data transfer capacity equal to or greater than 95th percentile traffic at 100 Megabits-per-second (Mbps). The Contractor shall ensure at least 30% of these Tor relays are operational within 60 days of award of this contract, at least 60% operational within 90 days of award, and the remainder operational within 120 days of award.

C.2.2 The Contractor shall provide and operate, either directly or by subcontracting, 75 Tor bridge servers, using leased cloud virtual servers or dedicated hosting services, with a total aggregate bandwidth (burst capacity) of no less than 7.5 Gigabits-per-second (Gbps) and monthly data transfer capacity equal to or greater than 95th percentile traffic at 100 Megabits-per-second (Mbps). The Contractor shall ensure at least 30% of these Tor bridges are operational within 60 days of award of this contract, at least 60% operational within 90 days of award, and the remainder operational within 120 days of award.

C.2.3 In order to provide additional capacity, improved performance, and enhanced security for BBG users of the Tor software in countries with government-imposed Internet censorship, the Contractor shall ensure that all Tor relay servers and Tor bridge servers operated under the terms of this contract (as per C.2.1 and C.2.2) shall be located in geographically diverse locations with diverse Internet Protocol (IP) addresses which are not in contiguous ranges in order to not be easily blocked by foreign government censors. To ensure diversity of IP addresses, no more than 2 servers may reside in the same /24 IP subnet, and to ensure geographical diversity, no more than 25 Tor relay servers or 7 Tor bridge servers may reside in the same data center, and at a minimum the Contractor must host servers across at least 1 data center facility in North America, 1 data center facility in Europe, and 1 data center facility in Asia.

C.2.4 The Contractor shall configure the Tor relays operated (per C.2.1) with an exit policy that at a minimum allows traffic destined for TCP ports 80, 443, 554, and 1755, and UDP ports 554 and 1755 to enable access to the world wide web and multimedia streaming. The Contractor may adopt a more permissive exit policy with the approval of the Contracting Officer's Technical Representative (COTR).

C.2.5 At the request of the COTR, the Contractor shall provide up to 12 customized versions of the Tor Browser Bundle software, which allow, at a minimum, for the default start page of the bundled web browser to be set to a URL as designated by the COTR for BBG services, as well as any further customizations as developed by the Contractor to promote the sponsorship and branding for BBG broadcasters, as approved by the COTR.

C.2.6 The Contractor shall track updates to the software components of the Tor Browser Bundle, and at no additional charge, produce and deliver updates to the customized versions (per C.2.5).

C.2.7 The Contractor shall test the Tor Browser Bundle on multiple computer systems, including all supported operating systems, and analyze these systems afterwards for any changes to the system that may have been made by use of the Tor Browser Bundle. The Contractor shall document any such traces found and design and deliver a plan with suggestions to reduce the footprint of Tor Browser Bundle use, as well as warnings and suggestions for Tor Browser Bundle end users to properly set security and privacy expectations for users.

C.2.8 The Contractor shall produce, release, and make available regular Tor package builds which are preconfigured to be a bridge relay.

C.2.9 The Contractor shall deliver a plan for additional Tor bridge deployment strategies, such as short-term browser-based bridges which allow volunteers to become Tor bridges without downloading any additional software.

C.2.10 OPTION: The Contractor shall evaluate the current Tor design and limitations on Tor relays which operate on dynamic IP addresses, and propose and with COTR approval implement technical improvements to reduce or remove these limitations.

C.2.11 OPTION: The Contractor shall design and implement technical improvements to Tor to allow Tor clients which meet acceptable criteria to be automatically promoted to become Tor relays upon explicit permission of the user running the Tor client.

C.2.12 OPTION: The Contractor shall design improvements to Torbutton to provide additional application layer security for Tor Browser Bundle users and improved support for streaming media in the Tor Browser Bundle.

for the Tor Browser Bundle, which integrates Adobe Flash into the sandboxed environment so that Tor Browser Bundle users can safely use Flash with Tor.

C.2.14 OPTION: The Contractor shall improve integration and usability of the HTTPS Everywhere extension for Firefox in the Tor Browser Bundle.

C.2.15 OPTION: The Contractor shall design a hardware-based network-attached device that will automatically run a Tor bridge with minimal configuration via a web-based user interface.

C.3 DELIVERABLES

C.3.1 The Contractor shall provide a Monthly Status Report no later than ten (10) business days after the end of each month to the COTR detailing work performed during the month. This report shall describe the work performed for specific requirements of this contract, including a detailed list of Tor relay servers and bridge servers operated (per C.2.1 and C.2.2), releases and promotion of Tor package builds preconfigured to be a bridge relay (per C.2.8), and status of any ongoing work for future deliverables including any exercised options.

C.3.2 The Contractor shall deliver to the COTR the customized versions of the Tor Browser Bundle software (per C.2.5). Each of the customized versions shall be prepared individually over the course of the contract period as directed by the COTR on an as-needed basis, the COTR may request multiple versions be prepared simultaneously, and all requests shall be fulfilled within ten (10) business days of each request. The Contractor shall deliver to the COTR updates to all customized versions within ten (10) business days of changes to the underlying version of the Tor Browser Bundle (per C.2.6).

C.3.3 The Contractor shall provide a detailed written report to the COTR of its analysis of traces left by the Tor Browser Bundle on various computer systems and its plan with suggestions to reduce the footprint of Tor Browser Bundle use (per C.2.7) no later than thirty (30) calendar days before the end of the initial period of performance for this contract.

C.3.4 The Contractor shall provide a detailed written report to the COTR of its plan for additional Tor bridge deployment strategies (per C.2.9) no later than thirty (30) calendar days before the end of the initial period of performance for this contract.

C.3.5 If option C.2.10 is exercised, the Contractor shall provide a detailed written report to the COTR with its proposed design to reduce or remove the limitations on Tor relays operating on dynamic IP addresses (per C.2.10) no later than thirty (30) days before the end of the period of performance for this contract in which the option is exercised.

C.3.6 If option C.2.11 is exercised, the Contractor shall provide a detailed written report to the COTR with its design to allow Tor clients to automatically be promoted to Tor relays (per C.2.11). With COTR approval, the Contractor shall deliver source code implementing these modifications to the Tor software no later than thirty (30) days before the end of the period of performance for this contract in which the option is exercised. Additionally, the Contractor shall submit its source code for those improvements to the Tor source code repository maintained by the Tor Project for consideration for inclusion in the mainline Tor software, per the current procedures as designated by the Tor Project, however this portion of the deliverable shall be considered fulfilled upon submission regardless of the acceptance of the Contractor's code by the Tor Project.

s design to improve Torbutton to provide additional application layer security and improved streaming media support for Tor Browser Bundle users (per C.2.12) no later than thirty (30) days before the end of the period of performance for this contract in which the option is exercised.

C.3.8 If option C.2.13 is exercised, the Contractor shall provide a detailed written report to the COTR with its design for a security sandbox for the Tor Browser Bundle which integrates Adobe Flash (per C.2.13), as well as source code implementing those modifications to the Tor software no later than thirty (30) days before the end of the period of performance for this contract in which the option is exercised. Additionally, the Contractor shall submit its source code for those modifications to the Tor source code repository maintained by the Tor Project for consideration for inclusion in the mainline Tor software, per the current procedures as designated by the Tor Project, however this portion of the deliverable shall be considered fulfilled upon submission regardless of the acceptance of the Contractor's code by the Tor Project.

C.3.9 If option C.2.14 is exercised, the Contractor shall provide a detailed written report to the COTR with its design to improve integration and usability of the HTTPS Everywhere extension for Firefox in the Tor Browser Bundle (per C.2.14) no later than thirty (30) days before the end of the period of performance for this contract in which the option is exercised.

C.3.10 If option C.2.15 is exercised, the Contractor shall provide a detailed written report to the COTR with its design for a hardware-based network-attached device to automatically run a Tor bridge (per C.2.15) no later than thirty (30) days before the end of the period of performance for this contract in which the option is exercised. This report must include full hardware and software specifications; suggested hardware vendors, model numbers, part numbers, and costs; detailed lists of operating system, and existing application software used, as well as any custom software which must be written to support the device.

C.4 ADDITIONAL TERMS

C.4.1 The Contractor shall be available for a telephone conference call with the COTR, other BBG staff and representatives at a mutually agreeable time on a periodic basis averaging no more than 2 calls per month of one hour's duration. This requirement is in addition to any other required communication by telephone or email with the COTR for execution of this contract.

C.4.2 All software and accompanying documentation developed under the terms of this contract must be distributed under an open source software license, such as the "BSD License" (http://www.opensource.org/licenses/bsd-license.php) or other commonly accepted open source software license as mutually agreed upon by the Contractor and the COTR. Any modifications to software already available under an open source software license must be licensed under the existing license terms.

COSTS

Cost of 12-month contract per terms above	$775,600
Cost for option tasks	$1,060,300
Total	$1,835,900

OPTION: Cost of optional improvements to allow Tor relays to operate on dynamic IP addresses (per C.2.10)
$ 126,00

OPTION: Cost of optional improvements to allow Tor clients to be automatically promoted to become Tor relays (per C.2.11)

$94,500

OPTION: Cost of optional improvements to Torbutton to improve security and media streaming (per C.2.12)

$100,800

OPTION: Cost of optional improvements to safe use of Flash within Tor (per C.2.13)

$ 189,000

OPTION: Cost of optional improvements to HTTPS Everywhere extension (per C.2.14)

$50,000

OPTION: Cost of optional dcvelopment of hardware-based network-attached device to pre-configured to run as a Tor bridge (per C.2.15)

$500,000

COST for OPTIONAL EXTENSIONS

Cost of additional 12-month contract extension (option year 1) per terms above $853,160

Cost of additional 12-month contract extension (option year 2) per terms above $938,476

Cost of additional 12-month contract extension (option year 3) per terms above $1,032,324

Cost of additional 12-month contract extension (option year 4) per terms above $1,135,556

Packaging and Marking

Inspection and Acceptance

Deliveries or Performance

PERIOD OF PERFORMANCE

ITEM	START	END
1	06/18/2012	06/17/2013

PERIOD OF PERFORMANCE

ITEM	START	END
2	06/18/2012	06/17/2013

PERIOD OF PERFORMANCE

ITEM	START	END
3	09/18/2012	09/17/2013

PERIOD OF PERFORMANCE

ITEM	START	END
4	09/18/2012	09/17/2013

PERIOD OF PERFORMANCE

ITEM	START	END
5	09/18/2012	09/17/2013

PERIOD OF PERFORMANCE

ITEM	START	END
6	09/18/2012	09/17/2013

Contract Administration Data
Accounting Data

Special Contract Requirements

Contract Clauses

Exhibits and Attachments TOC

Identifier	Title	Date	Number of Pages
2	Attachment: Statement of Work - BBG50-D-11-0061	09/01/2011	7

ORDER FOR SUPPLIES OR SERVICES

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

1. DATE OF ORDER
06/18/2012

2. CONTRACT NO. (If any)
BBG50-D-11-0061

3. ORDER NO.
BBG50-J-12-0508

4. REQUISITION/REFERENCE NO.
See Lines

5. ISSUING OFFICE (Address correspondence to)
Broadcasting Board of Governors, Office Of Contracts, 330 C Street SW, Room 4300, Washington, DC 20237

6. SHIP TO:

a. NAME OF CONSIGNEE
Malita Dyson

b. STREET ADDRESS
BBG Office of Engineering and Technical Services, 330 Independence Ave

c. CITY
Washington

d. STATE
DC

e. ZIP CODE
20237

f. SHIP VIA

7. TO:

a. NAME OF CONTRACTOR
TOR SOLUTIONS CORPORATION

b. COMPANY NAME
TOR SOLUTIONS CORPORATION

c. STREET ADDRESS
969 MAIN STREET, SUITE 206

d. CITY
WALPOLE

e. STATE
MA

f. ZIP CODE
02081-2972

8. TYPE OF ORDER

□ a. PURCHASE
REFERENCE YOUR:
Please furnish the following on the terms and conditions specified on both sides of this order and on the attached sheet, if any, including delivery as indicated.

□ b. DELIVERY -- Except for billing instructions on the reverse, this delivery order is subject to instructions contained on this side only of this form and is issued subject to the terms and conditions of the above-numbered contract.

9. ACCOUNTING AND APPROPRIATION DATA
See Line Item Detail

10. REQUISITIONING OFFICE
KELLY DEYOE, BBG Office of Engineering and Technical Services, 330 Independence Ave SW, Room 4301, Washington, DC 20237

11. BUSINESS CLASSIFICATION (Check appropriate box(es))
□ a. SMALL □ b. OTHER THAN SMALL □ c. DISADVANTAGED
□ d. WOMEN-OWNED □ e. HUBZone □ f. SERVICE-DISABLED VETERAN-OWNED

12. F.O.B. POINT

13. PLACE OF
a. INSPECTION
b. ACCEPTANCE

14. GOVERNMENT B/L NO.

15. DELIVER TO F.O.B. POINT ON OR BEFORE (Date)

16. DISCOUNT TERMS
0 Days: 0.00 %
0 Days: 0.00 %
0 Days: 0.00 %
0 Days: 0.00 %

17. SCHEDULE (See reverse for Rejections)

Item No. (a)	SUPPLIES OR SERVICES (b)	ORDERED QUANTITY (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
	See Lines					

SEE BILLING INSTRUCTIONS ON REVERSE

18. SHIPPING POINT

19. GROSS SHIPPING WEIGHT

20. INVOICE NO.

$775,600.20 17(h) TOT. (Cont. pages)

21. MAIL INVOICE TO:

a. NAME
Malita Dyson

b. STREET ADDRESS(or P.O. Box)
BBG Office of Engineering and Technical Services, 330 Independence Ave SW, Room 4300

c. CITY
Washington

d. STATE
DC

e. ZIP CODE
20237

$775,600.20 17(i) GRAND TOTAL

22. UNITED STATES OF AMERICA BY (Signature)
(b) (6) for

23. NAME (Typed)
Diane Sturgis
TITLE: CONTRACTING/ORDERING OFFICER

AUTHORIZED FOR LOCAL REPRODUCTION
PREVIOUS EDITION NOT USABLE

Generated by: AMS

SUPPLEMENTAL INVOICING INFORMATION

If desired, this order (or a copy thereof) may be used by the Contractor as the Contractor's invoice, instead of a separate invoice, provided the following statement, (signed and dated) is on (or attached to) the order: "Payment is requested in the amount of $_______. No other invoice will be submitted." However, if the Contractor wishes to submit an invoice, the following information must be provided; contract number (if any), order number, item number(s), description of supplies or service, sizes, quantities, unit prices, and extended totals. Prepaid shipping costs will be indicated as a separate item on the invoice. Where shipping costs exceed $10 (except for parcel post), the billing must be supported by a bill of lading or receipt. When several orders are invoiced to an ordering activity during the same billing period, consolidated periodic billings are encouraged.

RECEIVING REPORT

Quantity in the "Quantity Accepted" column on the face of this order has been: □ inspected, □ accepted, □ received by me and conforms to contract. Items listed below have been rejected for the reasons indicated.

SHIPMENT NUMBER	PARTIAL		DATE RECEIVED	SIGNATURE OF AUTHORIZED U.S. GOV'T REP.	DATE
	FINAL				
TOTAL CONTAINERS		GROSS WEIGHT	RECEIVED AT	TITLE	

REPORT OF REJECTIONS

ITEM NO.	SUPPLIES OR SERVICES	UNIT	QUANTITY REJECTED	REASON FOR REJECTION

Table of Contents

Summary Info Continuation Page
Continuation Sheet

Number	Quantity	Unit of Issue	Unit Price	Total Cost (+Inc. disc and tax)
1	Total : 12.000000	EA	Total: $25,000.0000	Total: $300,000.00

Period of Performance: 06/18/2012 - 06/17/2013
Description: This is an IDIQ {Referencing BBG50-D-11-0061} for Task 5 for the Peer-to-Peer with TOR. (SEE STATEMENT OF WORK)

Extended Description:

Delivery Schedule:

Delivery Number	Delivery Date	Quantity

Purchase Request Reference Line:T013-12-IQ-00038 - 0

Contract/BPA Number:BBG50-D-11-0061 - 1

1.
2012-0206-TSI-T013-4335-2544-250200
Total: $300,000.00

Number	Quantity	Unit of Issue	Unit Price	Total Cost (+Inc. disc and tax)
2	Total : 12.000000	YR	Total: $39,633.3500	Total: $475,600.20

Period of Performance: 06/18/2012 - 06/17/2013
Description: This is a requisition for TOR expansion Task #5 under the IDIQ. BBG50-D-11-61 See Attached for SOW

Extended Description:

Delivery Schedule:

Delivery Number	Delivery Date	Quantity

Purchase Request Reference Line:E013-12-IQ-00005 - 0

Contract/BPA Number:BBG50-D-11-0061 - 1

1.
2011-2012-0206-ENG-E013-4335-2544-454000-2011
Total: $475,600.20

Accounting Line Accounting and Appropriations Data:

Accounting and Funding Total:

Grand Total: $775,600.20

IDC Constraints Line Item

Line Number	Minumum Quantity	Minimum Amount	Maximum Quantity	Maximum Amount
1	0.000000	$0.00	0.000000	$0.00
2	0.000000	$0.00	0.000000	$0.00

Descriptions & Specifications
IDC Constraints Document

1000 STATEMENT OF WORK

SECTION C

DESCRIPTION/SPECIFICATIONS/STATEMENT OF WORK

C.1 BACKGROUND

The Broadcasting Board of Governors (BBG) oversees the mission and operation of several overseas broadcasting entities of the United States Government (USG). The International Broadcasting Bureau (IBB) oversees the daily operations of several USG broadcasters, including the Voice of America (VOA), and is responsible for all contractual and fiscal matters pertaining to broadcast operations. The IBB's Internet anti-censorship program seeks to ensure Internet users in target countries are able to access USG broadcasters' web sites to access their news and other programming, using a variety of tools to counter foreign government-sponsored Internet censorship controls.

This Statement of Work defines those duties the Contractor shall perform to enable the IBB to meet its goals of using Tor as a tool to further its Internet anti-censorship efforts. Tor is open source software, Tor and related software source code and binaries are available as free downloads from https://www.torproject.org/projects/projects.html.en and the source code can be freely modified to meet the requirements of this SOW (per the license terms contained on the project pages on the Tor Project web site).

C.2 TECHNICAL REQUIREMENTS

C.2.1 The Contractor shall provide and operate, either directly or by subcontracting, 125 Tor relay servers, using leased cloud virtual servers or dedicated hosting services, with a total aggregate bandwidth (burst capacity) of no less than 12.5 Gigabits-per-second (Gbps) and monthly data transfer capacity equal to or greater than 95th percentile traffic at 100 Megabits-per-second (Mbps). The Contractor shall ensure at least 30% of these Tor relays are operational within 60 days of award of this contract, at least 60% operational within 90 days of award, and the remainder operational within 120 days of award.

C.2.2 The Contractor shall provide and operate, either directly or by subcontracting, 75 Tor bridge servers, using leased cloud virtual servers or dedicated hosting services, with a total aggregate bandwidth (burst capacity) of no less than 7.5 Gigabits-per-second (Gbps) and monthly data transfer capacity equal to or greater than 95th percentile traffic at 100 Megabits-per-second (Mbps). The Contractor shall ensure at least 30% of these Tor bridges are operational within 60 days of award of this contract, at least 60% operational within 90 days of award, and the remainder operational within 120 days of award.

C.2.3 In order to provide additional capacity, improved performance, and enhanced security for BBG users of the Tor software in countries with government-imposed Internet censorship, the Contractor shall ensure that all Tor relay servers and Tor bridge servers operated under the terms of this contract (as per C.2.1 and C.2.2) shall be located in geographically diverse locations with diverse Internet Protocol (IP) addresses which are not in contiguous ranges in order to not be easily blocked by foreign government censors. To ensure diversity of IP addresses, no more than 2 servers may reside in the same /24 IP subnet, and to ensure geographical diversity, no more than 25 Tor relay servers or 7 Tor bridge servers may reside in the same data center, and at a minimum the Contractor must host servers across at least 1 data center facility in North America, 1 data center facility in Europe, and 1 data center facility in Asia.

C.2.4 The Contractor shall configure the Tor relays operated (per C.2.1) with an exit policy that at a minimum allows traffic destined for TCP ports 80, 443, 554, and 1755, and UDP ports 554 and 1755 to enable access to the world wide web and multimedia streaming. The Contractor may adopt a more permissive exit policy with the approval of the Contracting Officer's Technical Representative (COTR).

C.2.5 At the request of the COTR, the Contractor shall provide up to 12 customized versions of the Tor Browser Bundle software, which allow, at a minimum, for the default start page of the bundled web browser to be set to a URL as designated by the COTR for BBG services, as well as any further customizations as developed by the Contractor to promote the sponsorship and branding for BBG broadcasters, as approved by the COTR.

C.2.6 The Contractor shall track updates to the software components of the Tor Browser Bundle, and at no additional charge, produce and deliver updates to the customized versions (per C.2.5).

C.2.7 The Contractor shall test the Tor Browser Bundle on multiple computer systems, including all supported operating systems, and analyze these systems afterwards for any changes to the system that may have been made by use of the Tor Browser Bundle. The Contractor shall document any such traces found and design and deliver a plan with suggestions to reduce the footprint of Tor Browser Bundle use, as well as warnings and suggestions for Tor Browser Bundle end users to properly set security and privacy expectations for users.

C.2.8 The Contractor shall produce, release, and make available regular Tor package builds which are preconfigured to be a bridge relay.

C.2.9 The Contractor shall deliver a plan for additional Tor bridge deployment strategies, such as short-term browser-based bridges which allow volunteers to become Tor bridges without downloading any additional software.

C.2.10 OPTION: The Contractor shall evaluate the current Tor design and limitations on Tor relays which operate on dynamic IP addresses, and propose and with COTR approval implement technical improvements to reduce or remove these limitations.

C.2.11 OPTION: The Contractor shall design and implement technical improvements to Tor to allow Tor clients which meet acceptable criteria to be automatically promoted to become Tor relays upon explicit permission of the user running the Tor client.

C.2.12 OPTION: The Contractor shall design improvements to Torbutton to provide additional application layer security for Tor Browser Bundle users and improved support for streaming media in the Tor Browser Bundle.

C.2.13 OPTION: The Contractor shall design, and with COTR approval shall implement, a security sandbox for the Tor Browser Bundle, which integrates Adobe Flash into the sandboxed environment so that Tor Browser Bundle users can safely use Flash with Tor.

C.2.14 OPTION: The Contractor shall improve integration and usability of the HTTPS Everywhere extension for Firefox in the Tor Browser Bundle.

C.2.15 OPTION: The Contractor shall design a hardware-based network-attached device that will automatically run a Tor bridge with minimal configuration via a web-based user interface.

C.3 DELIVERABLES

C.3.1 The Contractor shall provide a Monthly Status Report no later than ten (10) business days after the end of each month to the COTR detailing work performed during the month. This report shall describe the work performed for specific requirements of this contract, including a detailed list of Tor relay servers and bridge servers operated (per C.2.1 and C.2.2), releases and promotion of Tor package builds preconfigured to be a bridge relay (per C.2.8), and status of any ongoing work for future deliverables including any exercised options.

C.3.2 The Contractor shall deliver to the COTR the customized versions of the Tor Browser Bundle software (per C.2.5). Each of the customized versions shall be prepared individually over the course of the contract period as directed by the COTR on an as-needed basis, the COTR may request multiple versions be prepared simultaneously, and all requests shall be fulfilled within ten (10) business days of each request. The Contractor shall deliver to the COTR updates to all customized versions within ten (10) business days of changes to the underlying version of the Tor Browser Bundle (per C.2.6).

C.3.3 The Contractor shall provide a detailed written report to the COTR of its analysis of traces left by the Tor Browser Bundle on various computer systems and its plan with suggestions to reduce the footprint of Tor Browser Bundle use (per C.2.7) no later than thirty (30) calendar days before the end of the initial period of performance for this contract.

C.3.4 The Contractor shall provide a detailed written report to the COTR of its plan for additional Tor bridge deployment strategies (per C.2.9) no later than thirty (30) calendar days before the end of the initial period of performance for this contract.

C.3.5 If option C.2.10 is exercised, the Contractor shall provide a detailed written report to the COTR with its proposed design to reduce or remove the limitations on Tor relays operating on dynamic IP addresses (per C.2.10) no later than thirty (30) days before the end of the period of performance for this contract in which the option is exercised.

C.3.6 If option C.2.11 is exercised, the Contractor shall provide a detailed written report to the COTR with its design to allow Tor clients to automatically be promoted to Tor relays (per C.2.11). With COTR approval, the Contractor shall deliver source code implementing these modifications to the Tor software no later than thirty (30) days before the end of the period of performance for this contract in which the option is exercised. Additionally, the Contractor shall submit its source code for those improvements to the Tor source code repository maintained by the Tor Project for consideration for inclusion in the mainline Tor software, per the current procedures as designated by the Tor Project, however this portion of the deliverable shall be considered fulfilled upon submission regardless of the acceptance of the Contractor's code by the Tor Project.

C.3.7 If option C.2.12 is exercised, the Contractor shall provide a detailed written report to the COTR with its design to improve Torbutton to provide additional application layer security and improved streaming media support for Tor Browser Bundle users (per C.2.12) no later than thirty (30) days before the end of the period of performance for this contract in which the option is exercised.

C.3.8 If option C.2.13 is exercised, the Contractor shall provide a detailed written report to the COTR with its design for a security sandbox for the Tor Browser Bundle which integrates Adobe Flash (per C.2.13), as well as source code implementing those modifications to the Tor software no later than thirty (30) days before the end of the period of performance for this contract in which the option is exercised. Additionally, the Contractor shall submit its source code for those modifications to the Tor source code repository maintained by the Tor Project for consideration for inclusion in the mainline Tor software, per the current procedures as designated by the Tor Project, however this portion of the deliverable shall be considered fulfilled upon submission regardless of the acceptance of the Contractor's code by the Tor Project.

C.3.9 If option C.2.14 is exercised, the Contractor shall provide a detailed written report to the COTR with its design to improve integration and usability of the HTTPS Everywhere extension for Firefox in the Tor Browser Bundle (per C.2.14) no later than thirty (30) days before the end of the period of performance for this contract in which the option is exercised.

C.3.10 If option C.2.15 is exercised, the Contractor shall provide a detailed written report to the COTR with its design for a hardware-based network-attached device to automatically run a Tor bridge (per C.2.15) no later than thirty (30) days before the end of the period of performance for this contract in which the option is exercised. This report must include full hardware and software specifications; suggested hardware vendors, model numbers, part numbers, and costs; detailed lists of operating system, and existing application software used, as well as any custom software which must be written to support the device.

C.4 ADDITIONAL TERMS

C.4.1 The Contractor shall be available for a telephone conference call with the COTR, other BBG staff and representatives at a mutually agreeable time on a periodic basis averaging no more than 2 calls per month of one hour's duration. This requirement is in addition to any other required communication by telephone or email with the COTR for execution of this contract.

C.4.2 All software and accompanying documentation developed under the terms of this contract must be distributed under an open source software license, such as the "BSD License" (http://www.opensource.org/licenses/bsd-license.php) or other commonly accepted open source software license as mutually agreed upon by the Contractor and the COTR. Any modifications to software already available under an open source software license must be licensed under the existing license terms.

COSTS

Cost of 12-month contract per terms above	$775,600
Cost for option tasks	$1,060,300
Total	$1,835,900

OPTION: Cost of optional improvements to allow Tor relays to operate on dynamic IP addresses (per C.2.10)

$ 126,00

OPTION: Cost of optional improvements to allow Tor clients to be automatically promoted to become Tor relays (per C.2.11)

$94,500

OPTION: Cost of optional improvements to Torbutton to improve security and media streaming (per C.2.12)

$100,800

OPTION: Cost of optional improvements to safe use of Flash within Tor (per C.2.13)

$ 189,000

OPTION: Cost of optional improvements to HTTPS Everywhere extension (per C.2.14)

$50,000

OPTION: Cost of optional development of hardware-based network-attached device to pre-configured to run as a Tor bridge (per C.2.15)

$500,000

COST for OPTIONAL EXTENSIONS

Cost of additional 12-month contract extension (option year 1) per terms above $853,160

Cost of additional 12-month contract extension (option year 2) per terms above $938,476

Cost of additional 12-month contract extension (option year 3) per terms above $1,032,324

Cost of additional 12-month contract extension (option year 4) per terms above $1,135,556

Packaging and Marking

Inspection and Acceptance

Deliveries or Performance

PERIOD OF PERFORMANCE

ITEM	**START**	**END**
1	06/18/2012	06/17/2013

PERIOD OF PERFORMANCE

ITEM	START	END
2	06/18/2012	06/17/2013

Contract Administration Data
Accounting Data

Special Contract Requirements

Contract Clauses

Exhibits and Attachments TOC

Identifier	Title	Date	Number of Pages
2	Attachment: Statement of Work - BBG50-D-11-0061	09/01/2011	7

Design of a blocking-resistant anonymity system DRAFT

Roger Dingledine and Nick Mathewson

The Free Haven Project
{arma,nickm}@freehaven.net

Abstract. Internet censorship is on the rise as websites around the world are increasingly blocked by government-level firewalls. Although popular anonymizing networks like Tor were originally designed to keep attackers from tracing people's activities, many people are also using them to evade local censorship. But if the censor simply denies access to the Tor network itself, blocked users can no longer benefit from the security Tor offers.
Here we describe a design that builds upon the current Tor network to provide an anonymizing network that resists blocking by government-level attackers.

1 Introduction and Goals

Anonymizing networks like Tor [11] bounce traffic around a network of encrypting relays. Unlike encryption, which hides only *what* is said, these networks also aim to hide who is communicating with whom, which users are using which websites, and similar relations. These systems have a broad range of users, including ordinary citizens who want to avoid being profiled for targeted advertisements, corporations who don't want to reveal information to their competitors, and law enforcement and government intelligence agencies who need to do operations on the Internet without being noticed.

Historical anonymity research has focused on an attacker who monitors the user (call her Alice) and tries to discover her activities, yet lets her reach any piece of the network. In more modern threat models such as Tor's, the adversary is allowed to perform active attacks such as modifying communications to trick Alice into revealing her destination, or intercepting some connections to run a man-in-the-middle attack. But these systems still assume that Alice can eventually reach the anonymizing network.

An increasing number of users are using the Tor software less for its anonymity properties than for its censorship resistance properties—if they use Tor to access Internet sites like Wikipedia and Blogspot, they are no longer affected by local censorship and firewall rules. In fact, an informal user study showed China as the third largest user base for Tor clients, with perhaps ten thousand people accessing the Tor network from China each day.

The current Tor design is easy to block if the attacker controls Alice's connection to the Tor network—by blocking the directory authorities, by blocking all the server IP addresses in the directory, or by filtering based on the fingerprint of the Tor TLS handshake. Here we describe an extended design that builds upon the current Tor network to provide an anonymizing network that resists censorship as well as anonymity-breaking attacks. In section 2 we discuss our threat model—that is, the assumptions we make about our adversary. Section 3 describes the components of the current Tor design and how they can be leveraged for a new blocking-resistant design. Section 4 explains the features and drawbacks of the currently deployed solutions. In sections 5 through 7, we explore the components of our designs in detail. Section 8 considers security implications and Section 9 presents other issues with maintaining connectivity and sustainability for the design. Section 10 speculates about future more complex designs, and finally Section 11 summarizes our next steps and recommendations.

2 Adversary assumptions

To design an effective anti-censorship tool, we need a good model for the goals and resources of the censors we are evading. Otherwise, we risk spending our effort on keeping the adversaries from doing things they have no interest in doing, and thwarting techniques they do not use. The history of blocking-resistance designs is littered with conflicting assumptions about what adversaries to expect and what problems are in the critical path to a solution. Here we describe our best understanding of the current situation around the world.

In the traditional security style, we aim to defeat a strong attacker—if we can defend against this attacker, we inherit protection against weaker attackers as well. After all, we want a general design that will work for citizens of China, Thailand, and other censored countries; for whistleblowers in firewalled corporate networks; and for people in unanticipated oppressive situations. In fact, by designing with a variety of adversaries in mind, we can take advantage of the fact that adversaries will be in different stages of the arms race at each location, so a server blocked in one locale can still be useful in others.

We assume that the attackers' goals are somewhat complex.

- The attacker would like to restrict the flow of certain kinds of information, particularly when this information is seen as embarrassing to those in power (such as information about rights violations or corruption), or when it enables or encourages others to oppose them effectively (such as information about opposition movements or sites that are used to organize protests).
- As a second-order effect, censors aim to chill citizens' behavior by creating an impression that their online activities are monitored.
- In some cases, censors make a token attempt to block a few sites for obscenity, blasphemy, and so on, but their efforts here are mainly for show. In other cases, they really do try hard to block such content.
- Complete blocking (where nobody at all can ever download censored content) is not a goal. Attackers typically recognize that perfect censorship is not only impossible, but unnecessary: if "undesirable" information is known only to a small few, further censoring efforts can be focused elsewhere.
- Similarly, the censors are not attempting to shut down or block *every* anti-censorship tool—merely the tools that are popular and effective (because these tools impede the censors' information restriction goals) and those tools that are highly visible (thus making the censors look ineffectual to their citizens and their bosses).
- Reprisal against *most* passive consumers of *most* kinds of blocked information is also not a goal, given the broadness of most censorship regimes. This seems borne out by fact.[1]
- Producers and distributors of targeted information are in much greater danger than consumers; the attacker would like to not only block their work, but identify them for reprisal.
- The censors (or their governments) would like to have a working, useful Internet. There are economic, political, and social factors that prevent them from "censoring" the Internet by outlawing it entirely, or by blocking access to all but a tiny list of sites. Nevertheless, the censors *are* willing to block innocuous content (like the bulk of a newspaper's reporting) in order to censor other content distributed through the same channels (like that newspaper's coverage of the censored country).

We assume there are three main technical network attacks in use by censors currently [7]:

[1] So far in places like China, the authorities mainly go after people who publish materials and coordinate organized movements [22]. If they find that a user happens to be reading a site that should be blocked, the typical response is simply to block the site. Of course, even with an encrypted connection, the adversary may be able to distinguish readers from publishers by observing whether Alice is mostly downloading bytes or mostly uploading them—we discuss this issue more in Section 8.2.

- Block a destination or type of traffic by automatically searching for certain strings or patterns in TCP packets. Offending packets can be dropped, or can trigger a response like closing the connection.
- Block a destination by listing its IP address at a firewall or other routing control point.
- Intercept DNS requests and give bogus responses for certain destination hostnames.

We assume the network firewall has limited CPU and memory per connection [7]. Against an adversary who could carefully examine the contents of every packet and correlate the packets in every stream on the network, we would need some stronger mechanism such as steganography, which introduces its own problems [15, 26]. But we make a "weak steganography" assumption here: to remain unblocked, it is necessary to remain unobservable only by computational resources on par with a modern router, firewall, proxy, or IDS.

We assume that while various different regimes can coordinate and share notes, there will be a time lag between one attacker learning how to overcome a facet of our design and other attackers picking it up. (The most common vector of transmission seems to be commercial providers of censorship tools: once a provider adds a feature to meet one country's needs or requests, the feature is available to all of the provider's customers.) Conversely, we assume that insider attacks become a higher risk only after the early stages of network development, once the system has reached a certain level of success and visibility.

We do not assume that government-level attackers are always uniform across the country. For example, users of different ISPs in China experience different censorship policies and mechanisms.

We assume that the attacker may be able to use political and economic resources to secure the cooperation of extraterritorial or multinational corporations and entities in investigating information sources. For example, the censors can threaten the service providers of troublesome blogs with economic reprisals if they do not reveal the authors' identities.

We assume that our users have control over their hardware and software—they don't have any spyware installed, there are no cameras watching their screens, etc. Unfortunately, in many situations these threats are real [28]; yet software-based security systems like ours are poorly equipped to handle a user who is entirely observed and controlled by the adversary. See Section 8.4 for more discussion of what little we can do about this issue.

Similarly, we assume that the user will be able to fetch a genuine version of Tor, rather than one supplied by the adversary; see Section 8.5 for discussion on helping the user confirm that he has a genuine version and that he can connect to the real Tor network.

3 Adapting the current Tor design to anti-censorship

Tor is popular and sees a lot of use—it's the largest anonymity network of its kind, and has attracted more than 800 volunteer-operated routers from around the world. Tor protects each user by routing their traffic through a multiply encrypted "circuit" built of a few randomly selected servers, each of which can remove only a single layer of encryption. Each server sees only the step before it and the step after it in the circuit, and so no single server can learn the connection between a user and her chosen communication partners. In this section, we examine some of the reasons why Tor has become popular, with particular emphasis to how we can take advantage of these properties for a blocking-resistance design.

Tor aims to provide three security properties:

- 1. A local network attacker can't learn, or influence, your destination.
- 2. No single router in the Tor network can link you to your destination.
- 3. The destination, or somebody watching the destination, can't learn your location.

For blocking-resistance, we care most clearly about the first property. But as the arms race progresses, the second property will become important—for example, to discourage an adversary from volunteering a relay in order to learn that Alice is reading or posting to certain websites. The third property helps keep users safe from collaborating websites: consider websites and other Internet services that have been pressured recently into revealing the identity of bloggers or treating clients differently depending on their network location [17].

The Tor design provides other features as well that are not typically present in manual or ad hoc circumvention techniques.

First, Tor has a well-analyzed and well-understood way to distribute information about servers. Tor directory authorities automatically aggregate, test, and publish signed summaries of the available Tor routers. Tor clients can fetch these summaries to learn which routers are available and which routers are suitable for their needs. Directory information is cached throughout the Tor network, so once clients have bootstrapped they never need to interact with the authorities directly. (To tolerate a minority of compromised directory authorities, we use a threshold trust scheme— see Section 8.5 for details.)

Second, the list of directory authorities is not hard-wired. Clients use the default authorities if no others are specified, but it's easy to start a separate (or even overlapping) Tor network just by running a different set of authorities and convincing users to prefer a modified client. For example, we could launch a distinct Tor network inside China; some users could even use an aggregate network made up of both the main network and the China network. (But we should not be too quick to create other Tor networks—part of Tor's anonymity comes from users behaving like other users, and there are many unsolved anonymity questions if different users know about different pieces of the network.)

Third, in addition to automatically learning from the chosen directories which Tor routers are available and working, Tor takes care of building paths through the network and rebuilding them as needed. So the user never has to know how paths are chosen, never has to manually pick working proxies, and so on. More generally, at its core the Tor protocol is simply a tool that can build paths given a set of routers. Tor is quite flexible about how it learns about the routers and how it chooses the paths. Harvard's Blossom project [16] makes this flexibility more concrete: Blossom makes use of Tor not for its security properties but for its reachability properties. It runs a separate set of directory authorities, its own set of Tor routers (called the Blossom network), and uses Tor's flexible path-building to let users view Internet resources from any point in the Blossom network.

Fourth, Tor separates the role of *internal relay* from the role of *exit relay*. That is, some volunteers choose just to relay traffic between Tor users and Tor routers, and others choose to also allow connections to external Internet resources. Because we don't force all volunteers to play both roles, we end up with more relays. This increased diversity in turn is what gives Tor its security: the more options the user has for her first hop, and the more options she has for her last hop, the less likely it is that a given attacker will be watching both ends of her circuit [11]. As a bonus, because our design attracts more internal relays that want to help out but don't want to deal with being an exit relay, we end up providing more options for the first hop—the one most critical to being able to reach the Tor network.

Fifth, Tor is sustainable. Zero-Knowledge Systems offered the commercial but now defunct Freedom Network [2], a design with security comparable to Tor's, but its funding model relied on collecting money from users to pay relay operators. Modern commercial proxy systems similarly need to keep collecting money to support their infrastructure. On the other hand, Tor has built a self-sustaining community of volunteers who donate their time and resources. This community trust is rooted in Tor's open design: we tell the world exactly how Tor works, and we provide all the source code. Users can decide for themselves, or pay any security expert to decide, whether it is safe to use. Further, Tor's modularity as described above, along with its open license, mean that its impact will continue to grow.

Sixth, Tor has an established user base of hundreds of thousands of people from around the world. This diversity of users contributes to sustainability as above: Tor is used by ordinary citizens, activists, corporations, law enforcement, and even government and military users, and they can only achieve their security goals by blending together in the same network [1, 9]. This user base also provides something else: hundreds of thousands of different and often-changing addresses that we can leverage for our blocking-resistance design.

Finally and perhaps most importantly, Tor provides anonymity and prevents any single server from linking users to their communication partners. Despite initial appearances, ***distributed-trust anonymity is critical for anti-censorship efforts.*** If any single server can expose dissident bloggers or compile a list of users' behavior, the censors can profitably compromise that server's operator, perhaps by applying economic pressure to their employers, breaking into their computer, pressuring their family (if they have relatives in the censored area), or so on. Furthermore, in designs where any relay can expose its users, the censors can spread suspicion that they are running some of the relays and use this belief to chill use of the network.

We discuss and adapt these components further in Section 5. But first we examine the strengths and weaknesses of other blocking-resistance approaches, so we can expand our repertoire of building blocks and ideas.

4 Current proxy solutions

Relay-based blocking-resistance schemes generally have two main components: a relay component and a discovery component. The relay part encompasses the process of establishing a connection, sending traffic back and forth, and so on—everything that's done once the user knows where she's going to connect. Discovery is the step before that: the process of finding one or more usable relays.

For example, we can divide the pieces of Tor in the previous section into the process of building paths and sending traffic over them (relay) and the process of learning from the directory servers about what routers are available (discovery). With this distinction in mind, we now examine several categories of relay-based schemes.

4.1 Centrally-controlled shared proxies

Existing commercial anonymity solutions (like Anonymizer.com) are based on a set of single-hop proxies. In these systems, each user connects to a single proxy, which then relays traffic between the user and her destination. These public proxy systems are typically characterized by two features: they control and operate the proxies centrally, and many different users get assigned to each proxy.

In terms of the relay component, single proxies provide weak security compared to systems that distribute trust over multiple relays, since a compromised proxy can trivially observe all of its users' actions, and an eavesdropper only needs to watch a single proxy to perform timing correlation attacks against all its users' traffic and thus learn where everyone is connecting. Worse, all users need to trust the proxy company to have good security itself as well as to not reveal user activities.

On the other hand, single-hop proxies are easier to deploy, and they can provide better performance than distributed-trust designs like Tor, since traffic only goes through one relay. They're also more convenient from the user's perspective—since users entirely trust the proxy, they can just use their web browser directly.

Whether public proxy schemes are more or less scalable than Tor is still up for debate: commercial anonymity systems can use some of their revenue to provision more bandwidth as they grow, whereas volunteer-based anonymity systems can attract thousands of fast relays to spread the load.

The discovery piece can take several forms. Most commercial anonymous proxies have one or a handful of commonly known websites, and their users log in to those websites and relay their traffic through them. When these websites get blocked (generally soon after the company becomes popular), if the company cares about users in the blocked areas, they start renting lots of disparate IP addresses and rotating through them as they get blocked. They notify their users of new addresses (by email, for example). It's an arms race, since attackers can sign up to receive the email too, but operators have one nice trick available to them: because they have a list of paying subscribers, they can notify certain subscribers about updates earlier than others.

Access control systems on the proxy let them provide service only to users with certain characteristics, such as paying customers or people from certain IP address ranges.

Discovery in the face of a government-level firewall is a complex and unsolved topic, and we're stuck in this same arms race ourselves; we explore it in more detail in Section 7. But first we examine the other end of the spectrum—getting volunteers to run the proxies, and telling only a few people about each proxy.

4.2 Independent personal proxies

Personal proxies such as Circumventor [18] and CGIProxy [23] use the same technology as the public ones as far as the relay component goes, but they use a different strategy for discovery. Rather than managing a few centralized proxies and constantly getting new addresses for them as the old addresses are blocked, they aim to have a large number of entirely independent proxies, each managing its own (much smaller) set of users.

As the Circumventor site explains, "You don't actually install the Circumventor *on* the computer that is blocked from accessing Web sites. You, or a friend of yours, has to install the Circumventor on some *other* machine which is not censored."

This tactic has great advantages in terms of blocking-resistance—recall our assumption in Section 2 that the attention a system attracts from the attacker is proportional to its number of users and level of publicity. If each proxy only has a few users, and there is no central list of proxies, most of them will never get noticed by the censors.

On the other hand, there's a huge scalability question that so far has prevented these schemes from being widely useful: how does the fellow in China find a person in Ohio who will run a Circumventor for him? In some cases he may know and trust some people on the outside, but in many cases he's just out of luck. Just as hard, how does a new volunteer in Ohio find a person in China who needs it?

This challenge leads to a hybrid design—centrally-distributed personal proxies—which we will investigate in more detail in Section 7.

4.3 Open proxies

Yet another currently used approach to bypassing firewalls is to locate open and misconfigured proxies on the Internet. A quick Google search for "open proxy list" yields a wide variety of freely available lists of HTTP, HTTPS, and SOCKS proxies. Many small companies have sprung up providing more refined lists to paying customers.

There are some downsides to using these open proxies though. First, the proxies are of widely varying quality in terms of bandwidth and stability, and many of them are entirely unreachable. Second, unlike networks of volunteers like Tor, the legality of routing traffic through these proxies is questionable: it's widely believed that most of them don't realize what they're offering, and probably wouldn't allow it if they realized. Third, in many cases the connection to the proxy is unencrypted, so firewalls that filter based on keywords in IP packets will not be hindered. Fourth, in many countries (including China), the firewall authorities hunt for open proxies as well, to preemptively block them. And last, many users are suspicious that some open proxies are a little *too* convenient: are they run by the adversary, in which case they get to monitor all the user's requests just as single-hop proxies can?

A distributed-trust design like Tor resolves each of these issues for the relay component, but a constantly changing set of thousands of open relays is clearly a useful idea for a discovery component. For example, users might be able to make use of these proxies to bootstrap their first introduction into the Tor network.

4.4 Blocking resistance and JAP

Köpsell and Hilling's Blocking Resistance design [20] is probably the closest related work, and is the starting point for the design in this paper. In this design, the JAP anonymity system [3] is used as a base instead of Tor. Volunteers operate a large number of access points that relay traffic to the core JAP network, which in turn anonymizes users' traffic. The software to run these relays is, as in our design, included in the JAP client software and enabled only when the user decides to enable it. Discovery is handled with a CAPTCHA-based mechanism; users prove that they aren't an automated process, and are given the address of an access point. (The problem of a determined attacker with enough manpower to launch many requests and enumerate all the access points is not considered in depth.) There is also some suggestion that information about access points could spread through existing social networks.

4.5 Infranet

The Infranet design [14] uses one-hop relays to deliver web content, but disguises its communications as ordinary HTTP traffic. Requests are split into multiple requests for URLs on the relay, which then encodes its responses in the content it returns. The relay needs to be an actual website with plausible content and a number of URLs which the user might want to access—if the Infranet software produced its own cover content, it would be far easier for censors to identify. To keep the censors from noticing that cover content changes depending on what data is embedded, Infranet needs the cover content to have an innocuous reason for changing frequently: the paper recommends watermarked images and webcams.

The attacker and relay operators in Infranet's threat model are significantly different than in ours. Unlike our attacker, Infranet's censor can't be bypassed with encrypted traffic (presumably because the censor blocks encrypted traffic, or at least considers it suspicious), and has more computational resources to devote to each connection than ours (so it can notice subtle patterns over time). Unlike our bridge operators, Infranet's operators (and users) have more bandwidth to spare; the overhead in typical steganography schemes is far higher than Tor's.

The Infranet design does not include a discovery element. Discovery, however, is a critical point: if whatever mechanism allows users to learn about relays also allows the censor to do so, he can trivially discover and block their addresses, even if the steganography would prevent mere traffic observation from revealing the relays' addresses.

4.6 RST-evasion and other packet-level tricks

In their analysis of China's firewall's content-based blocking, Clayton, Murdoch and Watson discovered that rather than blocking all packets in a TCP streams once a forbidden word was noticed, the firewall was simply forging RST packets to make the communicating parties believe that the connection was closed [7]. They proposed altering operating systems to ignore forged RST packets. This approach might work in some cases, but in practice it appears that many firewalls start filtering by IP address once a sufficient number of RST packets have been sent.

Other packet-level responses to filtering include splitting sensitive words across multiple TCP packets, so that the censors' firewalls can't notice them without performing expensive stream reconstruction [27]. This technique relies on the same insight as our weak steganography assumption.

4.7 Internal caching networks

Freenet [6] is an anonymous peer-to-peer data store. Analyzing Freenet's security can be difficult, as its design is in flux as new discovery and routing mechanisms are proposed, and no complete specification has (to our knowledge) been written. Freenet servers relay requests for specific content (indexed by a digest of the content) "toward" the server that hosts it, and then cache the content as it follows the same path back to the requesting user. If Freenet's routing mechanism is successful in allowing nodes to learn about each other and route correctly even as some node-to-node links are blocked by firewalls, then users inside censored areas can ask a local Freenet server for a piece of content, and get an answer without having to connect out of the country at all. Of course, operators of servers inside the censored area can still be targeted, and the addresses of external servers can still be blocked.

4.8 Skype

The popular Skype voice-over-IP software uses multiple techniques to tolerate restrictive networks, some of which allow it to continue operating in the presence of censorship. By switching ports and using encryption, Skype attempts to resist trivial blocking and content filtering. Even if no encryption were used, it would still be expensive to scan all voice traffic for sensitive words. Also, most current keyloggers are unable to store voice traffic. Nevertheless, Skype can still be blocked, especially at its central login server.

4.9 Tor itself

And last, we include Tor itself in the list of current solutions to firewalls. Tens of thousands of people use Tor from countries that routinely filter their Internet. Tor's website has been blocked in most of them. But why hasn't the Tor network been blocked yet?

We have several theories. The first is the most straightforward: tens of thousands of people are simply too few to matter. It may help that Tor is perceived to be for experts only, and thus not worth attention yet. The more subtle variant on this theory is that we've positioned Tor in the public eye as a tool for retaining civil liberties in more free countries, so perhaps blocking authorities don't view it as a threat. (We revisit this idea when we consider whether and how to publicize a Tor variant that improves blocking-resistance—see Section 9.5 for more discussion.)

The broader explanation is that the maintenance of most government-level filters is aimed at stopping widespread information flow and appearing to be in control, not by the impossible goal of blocking all possible ways to bypass censorship. Censors realize that there will always be ways for a few people to get around the firewall, and as long as Tor has not publically threatened their control, they see no urgent need to block it yet.

We should recognize that we're *already* in the arms race. These constraints can give us insight into the priorities and capabilities of our various attackers.

5 The relay component of our blocking-resistant design

Section 3 describes many reasons why Tor is well-suited as a building block in our context, but several changes will allow the design to resist blocking better. The most critical changes are to get more relay addresses, and to distribute them to users differently.

5.1 Bridge relays

Today, Tor servers operate on less than a thousand distinct IP addresses; an adversary could enumerate and block them all with little trouble. To provide a means of ingress to the network, we need a larger set of entry points, most of which an adversary won't be able to enumerate easily. Fortunately, we have such a set: the Tor users.

Hundreds of thousands of people around the world use Tor. We can leverage our already self-selected user base to produce a list of thousands of frequently-changing IP addresses. Specifically, we can give them a little button in the GUI that says "Tor for Freedom", and users who click the button will turn into *bridge relays* (or just *bridges* for short). They can rate limit relayed connections to 10 KB/s (almost nothing for a broadband user in a free country, but plenty for a user who otherwise has no access at all), and since they are just relaying bytes back and forth between blocked users and the main Tor network, they won't need to make any external connections to Internet sites. Because of this separation of roles, and because we're making use of software that the volunteers have already installed for their own use, we expect our scheme to attract and maintain more volunteers than previous schemes.

As usual, there are new anonymity and security implications from running a bridge relay, particularly from letting people relay traffic through your Tor client; but we leave this discussion for Section 8.

5.2 The bridge directory authority

How do the bridge relays advertise their existence to the world? We introduce a second new component of the design: a specialized directory authority that aggregates and tracks bridges. Bridge relays periodically publish server descriptors (summaries of their keys, locations, etc, signed by their long-term identity key), just like the relays in the "main" Tor network, but in this case they publish them only to the bridge directory authorities.

The main difference between bridge authorities and the directory authorities for the main Tor network is that the main authorities provide a list of every known relay, but the bridge authorities only give out a server descriptor if you already know its identity key. That is, you can keep up-to-date on a bridge's location and other information once you know about it, but you can't just grab a list of all the bridges.

The identity key, IP address, and directory port for each bridge authority ship by default with the Tor software, so the bridge relays can be confident they're publishing to the right location, and the blocked users can establish an encrypted authenticated channel. See Section 8.5 for more discussion of the public key infrastructure and trust chain.

Bridges use Tor to publish their descriptors privately and securely, so even an attacker monitoring the bridge directory authority's network can't make a list of all the addresses contacting the authority. Bridges may publish to only a subset of the authorities, to limit the potential impact of an authority compromise.

5.3 Putting them together

If a blocked user knows the identity keys of a set of bridge relays, and he has correct address information for at least one of them, he can use that one to make a secure connection to the bridge authority and update his knowledge about the other bridge relays. He can also use it to make secure connections to the main Tor network and directory servers, so he can build circuits and connect to the rest of the Internet. All of these updates happen in the background: from the blocked user's perspective, he just accesses the Internet via his Tor client like always.

So now we've reduced the problem from how to circumvent the firewall for all transactions (and how to know that the pages you get have not been modified by the local attacker) to how to learn about a working bridge relay.

There's another catch though. We need to make sure that the network traffic we generate by simply connecting to a bridge relay doesn't stand out too much.

6 Hiding Tor's network fingerprint

Currently, Tor uses two protocols for its network communications. The main protocol uses TLS for encrypted and authenticated communication between Tor instances. The second protocol is standard HTTP, used for fetching directory information. All Tor servers listen on their "ORPort" for TLS connections, and some of them opt to listen on their "DirPort" as well, to serve directory information. Tor servers choose whatever port numbers they like; the server descriptor they publish to the directory tells users where to connect.

One format for communicating address information about a bridge relay is its IP address and DirPort. From there, the user can ask the bridge's directory cache for an up-to-date copy of its server descriptor, and learn its current circuit keys, its ORPort, and so on.

However, connecting directly to the directory cache involves a plaintext HTTP request. A censor could create a network fingerprint (known as a *signature* in the intrusion detection field) for the request and/or its response, thus preventing these connections. To resolve this vulnerability, we've modified the Tor protocol so that users can connect to the directory cache via the main Tor port—they establish a TLS connection with the bridge as normal, and then send a special "begindir" relay command to establish an internal connection to its directory cache.

Therefore a better way to summarize a bridge's address is by its IP address and ORPort, so all communications between the client and the bridge will use ordinary TLS. But there are other details that need more investigation.

What port should bridges pick for their ORPort? We currently recommend that they listen on port 443 (the default HTTPS port) if they want to be most useful, because clients behind standard firewalls will have the best chance to reach them. Is this the best choice in all cases, or should we encourage some fraction of them pick random ports, or other ports commonly permitted through firewalls like 53 (DNS) or 110 (POP)? Or perhaps we should use other ports where TLS traffic is expected, like 993 (IMAPS) or 995 (POP3S). We need more research on our potential users, and their current and anticipated firewall restrictions.

Furthermore, we need to look at the specifics of Tor's TLS handshake. Right now Tor uses some predictable strings in its TLS handshakes. For example, it sets the X.509 organizationName field to "Tor", and it puts the Tor server's nickname in the certificate's commonName field. We should tweak the handshake protocol so it doesn't rely on any unusual details in the certificate, yet it remains secure; the certificate itself should be made to resemble an ordinary HTTPS certificate. We should also try to make our advertised cipher-suites closer to what an ordinary web server would support.

Tor's TLS handshake uses two-certificate chains: one certificate contains the self-signed identity key for the router, and the second contains a current TLS key, signed by the identity key. We use these to authenticate that we're talking to the right router, and to limit the impact of TLS-key exposure. Most (though far from all) consumer-oriented HTTPS services provide only a single certificate. These extra certificates may help identify Tor's TLS handshake; instead, bridges should consider using only a single TLS key certificate signed by their identity key, and providing the full value of the identity key in an early handshake cell. More significantly, Tor currently has all clients present certificates, so that clients are harder to distinguish from servers. But in a blocking-resistance environment, clients should not present certificates at all.

Last, what if the adversary starts observing the network traffic even more closely? Even if our TLS handshake looks innocent, our traffic timing and volume still look different than a user making a secure web connection to his bank. The same techniques used in the growing trend to build tools to recognize encrypted Bittorrent traffic could be used to identify Tor communication and recognize bridge relays. Rather than trying to look like encrypted web traffic, we may be better off trying to blend with some other encrypted network protocol. The first step is to compare typical network behavior for a Tor client to typical network behavior for various other protocols. This statistical cat-and-mouse game is made more complex by the fact that Tor transports a variety of protocols, and we'll want to automatically handle web browsing differently from, say, instant messaging.

6.1 Identity keys as part of addressing information

We have described a way for the blocked user to bootstrap into the network once he knows the IP address and ORPort of a bridge. What about local spoofing attacks? That is, since we never learned an identity key fingerprint for the bridge, a local attacker could intercept our connection and pretend to be the bridge we had in mind. It turns out that giving false information isn't that bad—since the Tor client ships with trusted keys for the bridge directory authority and the Tor network directory authorities, the user can learn whether he's being given a real connection to the bridge authorities or not. (After all, if the adversary intercepts every connection the user makes and gives him a bad connection each time, there's nothing we can do.)

What about anonymity-breaking attacks from observing traffic, if the blocked user doesn't start out knowing the identity key of his intended bridge? The vulnerabilities aren't so bad in this case either—the adversary could do similar attacks just by monitoring the network traffic.

Once the Tor client has fetched the bridge's server descriptor, it should remember the identity key fingerprint for that bridge relay. Thus if the bridge relay moves to a new IP address, the client can query the bridge directory authority to look up a fresh server descriptor using this fingerprint.

So we've shown that it's *possible* to bootstrap into the network just by learning the IP address and ORPort of a bridge, but are there situations where it's more convenient or more secure to learn the bridge's identity fingerprint as well as instead, while bootstrapping? We keep that question in mind as we next investigate bootstrapping and discovery.

7 Discovering working bridge relays

Tor's modular design means that we can develop a better relay component independently of developing the discovery component. This modularity's great promise is that we can pick any discovery approach we like; but the unfortunate fact is that we have no magic bullet for discovery. We're in the same arms race as all the other designs we described in Section 4.

In this section we describe a variety of approaches to adding discovery components for our design.

7.1 Bootstrapping: finding your first bridge.

In Section 5.3, we showed that a user who knows a working bridge address can use it to reach the bridge authority and to stay connected to the Tor network. But how do new users reach the bridge authority in the first place? After all, the bridge authority will be one of the first addresses that a censor blocks.

First, we should recognize that most government firewalls are not perfect. That is, they may allow connections to Google cache or some open proxy servers, or they let file-sharing traffic, Skype, instant messaging, or World-of-Warcraft connections through. Different users will have different mechanisms for bypassing the firewall initially. Second, we should remember that most people don't operate in a vacuum; users will hopefully know other people who are in other situations or have other resources available. In the rest of this section we develop a toolkit of different options and mechanisms, so that we can enable users in a diverse set of contexts to bootstrap into the system.

(For users who can't use any of these techniques, hopefully they know a friend who can—for example, perhaps the friend already knows some bridge relay addresses. If they can't get around it at all, then we can't help them—they should go meet more people or learn more about the technology running the firewall in their area.)

By deploying all the schemes in the toolkit at once, we let bridges and blocked users employ the discovery approach that is most appropriate for their situation.

7.2 Independent bridges, no central discovery

The first design is simply to have no centralized discovery component at all. Volunteers run bridges, and we assume they have some blocked users in mind and communicate their address information to them out-of-band (for example, through Gmail). This design allows for small personal bridges that have only one or a handful of users in mind, but it can also support an entire community of users. For example, Citizen Lab's upcoming Psiphon single-hop proxy tool [13] plans to use this *social network* approach as its discovery component.

There are several ways to do bootstrapping in this design. In the simple case, the operator of the bridge informs each chosen user about his bridge's address information and/or keys. A different approach involves blocked users introducing new blocked users to the bridges they know. That is, somebody in the blocked area can pass along a bridge's address to somebody else they trust. This scheme brings in appealing but complex game theoretic properties: the blocked user making the decision has an incentive only to delegate to trustworthy people, since an adversary who learns the bridge's address and filters it makes it unavailable for both of them. Also, delegating known bridges to members of your social network can be dangerous: an the adversary who can learn who knows which bridges may be able to reconstruct the social network.

Note that a central set of bridge directory authorities can still be compatible with a decentralized discovery process. That is, how users first learn about bridges is entirely up to the bridges, but the process of fetching up-to-date descriptors for them can still proceed as described in Section 5. Of course, creating a central place that knows about all the bridges may not be smart, especially if every other piece of the system is decentralized. Further, if a user only knows about one bridge and he loses track of it, it may be quite a hassle to reach the bridge authority. We address these concerns next.

7.3 Families of bridges, no central discovery

Because the blocked users are running our software too, we have many opportunities to improve usability or robustness. Our second design builds on the first by encouraging volunteers to run several bridges at once (or coordinate with other bridge volunteers), such that some of the bridges are likely to be available at any given time.

The blocked user's Tor client would periodically fetch an updated set of recommended bridges from any of the working bridges. Now the client can learn new additions to the bridge pool, and can expire abandoned bridges or bridges that the adversary has blocked, without the user ever needing to care. To simplify maintenance of the community's bridge pool, each community could run its own bridge directory authority—reachable via the available bridges, and also mirrored at each bridge.

7.4 Public bridges with central discovery

What about people who want to volunteer as bridges but don't know any suitable blocked users? What about people who are blocked but don't know anybody on the outside? Here we describe how to make use of these *public bridges* in a way that still makes it hard for the attacker to learn all of them.

The basic idea is to divide public bridges into a set of pools based on identity key. Each pool corresponds to a *distribution strategy*: an approach to distributing its bridge addresses to users. Each strategy is designed to exercise a different scarce resource or property of the user.

How do we divide bridges between these strategy pools such that they're evenly distributed and the allocation is hard to influence or predict, but also in a way that's amenable to creating more strategies later on without reshuffling all the pools? We assign a given bridge to a strategy pool by hashing the bridge's identity key along with a secret that only the bridge authority knows: the first n bits of this hash dictate the strategy pool number, where n is a parameter that describes how many strategy pools we want at this point. We choose $n = 3$ to start, so we divide bridges between 8 pools; but as we later invent new distribution strategies, we can increment n to split the 8 into 16. Since a bridge can't predict the next bit in its hash, it can't anticipate which identity key will correspond to a certain new pool when the pools are split. Further, since the bridge authority doesn't provide any feedback to the bridge about which strategy pool it's in, an adversary who signs up bridges with the goal of filling a certain pool [12] will be hindered.

The first distribution strategy (used for the first pool) publishes bridge addresses in a time-release fashion. The bridge authority divides the available bridges into partitions, and each partition is deterministically available only in certain time windows. That is, over the course of a given time slot (say, an hour), each requester is given a random bridge from within that partition. When the next time slot arrives, a new set of bridges from the pool are available for discovery. Thus some bridge address is always available when a new user arrives, but to learn about all bridges the attacker needs to fetch all new addresses at every new time slot. By varying the length of the time slots, we can make it harder for the attacker to guess when to check back. We expect these bridges will be the first to be blocked, but they'll help the system bootstrap until they *do* get blocked. Further, remember that we're dealing with different blocking regimes around the world that will progress at different rates—so this pool will still be useful to some users even as the arms races progress.

The second distribution strategy publishes bridge addresses based on the IP address of the requesting user. Specifically, the bridge authority will divide the available bridges in the pool into a bunch of partitions (as in the first distribution scheme), hash the requester's IP address with a secret of its own (as in the above allocation scheme for creating pools), and give the requester a random bridge from the appropriate partition. To raise the bar, we should discard the last octet of the IP address before inputting it to the hash function, so an attacker who only controls a single "/24" network only counts as one user. A large attacker like China will still be able to control many addresses, but the hassle of establishing connections from each network (or spoofing TCP connections) may still slow them down. Similarly, as a special case, we should treat IP addresses that are Tor exit nodes as all being on the same network.

The third strategy combines the time-based and location-based strategies to further constrain and rate-limit the available bridge addresses. Specifically, the bridge address provided in a given time slot to a given network location is deterministic within the partition, rather than chosen randomly each time from the partition. Thus, repeated requests during that time slot from a given network are given the same bridge address as the first request.

The fourth strategy is based on Circumventor's discovery strategy. The Circumventor project, realizing that its adoption will remain limited if it has no central coordination mechanism, has started a mailing list to distribute new proxy addresses every few days. From experimentation it seems they have concluded that sending updates every three or four days is sufficient to stay ahead of the current attackers.

The fifth strategy provides an alternative approach to a mailing list: users provide an email address and receive an automated response listing an available bridge address. We could limit one response per email address. To further rate limit queries, we could require a CAPTCHA solution in each case too. In fact, we wouldn't need to implement the CAPTCHA on our side: if we only deliver bridge addresses to Yahoo or GMail addresses, we can leverage the rate-limiting schemes that other parties already impose for account creation.

The sixth strategy ties in the social network design with public bridges and a reputation system. We pick some seeds—trusted people in blocked areas—and give them each a few dozen bridge addresses and a few *delegation tokens*. We run a website next to the bridge authority, where users can log in (they connect via Tor, and they don't need to provide actual identities, just persistent pseudonyms). Users can delegate trust to other people they know by giving them a token, which can be exchanged for a new account on the website. Accounts in "good standing" then accrue new bridge addresses and new tokens. As usual, reputation schemes bring in a host of new complexities [10]: how do we decide that an account is in good standing? We could tie reputation to whether the bridges they're told about have been blocked—see Section 7.7 below for initial thoughts on how to discover whether bridges have been blocked. We could track reputation between accounts (if you delegate to somebody who screws up, it impacts you too), or we could use blinded delegation tokens [5] to prevent the website from mapping the seeds' social network. We put off deeper discussion of the social network reputation strategy for future work.

Pools seven and eight are held in reserve, in case our currently deployed tricks all fail at once and the adversary blocks all those bridges—so we can adapt and move to new approaches quickly, and have some bridges immediately available for the new schemes. New strategies might be based on some other scarce resource, such as relaying traffic for others or other proof of energy spent. (We might also worry about the incentives for bridges that sign up and get allocated to the reserve pools: will they be unhappy that they're not being used? But this is a transient problem: if Tor users are bridges by default, nobody will mind not being used yet. See also Section 9.4.)

7.5 Public bridges with coordinated discovery

We presented the above discovery strategies in the context of a single bridge directory authority, but in practice we will want to distribute the operations over several bridge authorities—a single point of failure or attack is a bad move. The first answer is to run several independent bridge directory authorities, and bridges gravitate to one based on their identity key. The better answer would be some federation of bridge authorities that work together to provide redundancy but don't introduce new security issues. We could even imagine designs where the bridge authorities have encrypted versions of the bridge's server descriptors, and the users learn a decryption key that they keep private when they first hear about the bridge—this way the bridge authorities would not be able to learn the IP address of the bridges.

We leave this design question for future work.

7.6 Assessing whether bridges are useful

Learning whether a bridge is useful is important in the bridge authority's decision to include it in responses to blocked users. For example, if we end up with a list of thousands of bridges and only a few dozen of them are reachable right now, most blocked users will not end up knowing about working bridges.

There are three components for assessing how useful a bridge is. First, is it reachable from the public Internet? Second, what proportion of the time is it available? Third, is it blocked in certain jurisdictions?

The first component can be tested just as we test reachability of ordinary Tor servers. Specifically, the bridges do a self-test—connect to themselves via the Tor network—before they are willing to publish their descriptor, to make sure they're not obviously broken or misconfigured. Once the bridges publish, the bridge authority also tests reachability to make sure they're not confused or outright lying.

The second component can be measured and tracked by the bridge authority. By doing periodic reachability tests, we can get a sense of how often the bridge is available. More complex tests will involve bandwidth-intensive checks to force the bridge to commit resources in order to be counted as available. We need to evaluate how the relationship of uptime percentage should weigh into our choice of which bridges to advertise. We leave this to future work.

The third component is perhaps the trickiest: with many different adversaries out there, how do we keep track of which adversaries have blocked which bridges, and how do we learn about new blocks as they occur? We examine this problem next.

7.7 How do we know if a bridge relay has been blocked?

There are two main mechanisms for testing whether bridges are reachable from inside each blocked area: active testing via users, and passive testing via bridges.

In the case of active testing, certain users inside each area sign up as testing relays. The bridge authorities can then use a Blossom-like [16] system to build circuits through them to each bridge and see if it can establish the connection. But how do we pick the users? If we ask random users to do the testing (or if we solicit volunteers from the users), the adversary should sign up so he can enumerate the bridges we test. Indeed, even if we hand-select our testers, the adversary might still discover their location and monitor their network activity to learn bridge addresses.

Another answer is not to measure directly, but rather let the bridges report whether they're being used. Specifically, bridges should install a GeoIP database such as the public IP-To-Country list [19], and then periodically report to the bridge authorities which countries they're seeing use from. This data would help us track which countries are making use of the bridge design, and can also let us learn about new steps the adversary has taken in the arms race. (The compressed GeoIP database is only several hundred kilobytes, and we could even automate the update process by serving it from the bridge authorities.) More analysis of this passive reachability testing design is needed to resolve its many edge cases: for example, if a bridge stops seeing use from a certain area, does that mean the bridge is blocked or does that mean those users are asleep?

There are many more problems with the general concept of detecting whether bridges are blocked. First, different zones of the Internet are blocked in different ways, and the actual firewall jurisdictions do not match country borders. Our bridge scheme could help us map out the topology of the censored Internet, but this is a huge task. More generally, if a bridge relay isn't reachable, is that because of a network block somewhere, because of a problem at the bridge relay, or just a temporary outage somewhere in between? And last, an attacker could poison our bridge database by signing up already-blocked bridges. In this case, if we're stingy giving out bridge addresses, users in that country won't learn working bridges.

All of these issues are made more complex when we try to integrate this testing into our social network reputation system above. Since in that case we punish or reward users based on whether bridges get blocked, the adversary has new attacks to trick or bog down the reputation tracking. Indeed, the bridge authority doesn't even know what zone the blocked user is in, so do we blame him for any possible censored zone, or what?

Clearly more analysis is required. The eventual solution will probably involve a combination of passive measurement via GeoIP and active measurement from trusted testers. More generally, we can use the passive feedback mechanism to track usage of the bridge network as a whole—which would let us respond to attacks and adapt the design, and it would also let the general public track the progress of the project.

7.8 Advantages of deploying all solutions at once

For once, we're not in the position of the defender: we don't have to defend against every possible filtering scheme; we just have to defend against at least one. On the flip side, the attacker is forced to guess how to allocate his resources to defend against each of these discovery strategies. So by deploying all of our strategies at once, we not only increase our chances of finding one that the adversary has difficulty blocking, but we actually make *all* of the strategies more robust in the face of an adversary with limited resources.

8 Security considerations

8.1 Possession of Tor in oppressed areas

Many people speculate that installing and using a Tor client in areas with particularly extreme firewalls is a high risk—and the risk increases as the firewall gets more restrictive. This notion certain has merit, but there's a counter pressure as well: as the firewall gets more restrictive, more ordinary people behind it end up using Tor for more mainstream activities, such as learning about Wall Street prices or looking at pictures of women's ankles. So as the restrictive firewall pushes up the number of Tor users, the "typical" Tor user becomes more mainstream, and therefore mere use or possession of the Tor software is not so surprising.

It's hard to say which of these pressures will ultimately win out, but we should keep both sides of the issue in mind.

8.2 Observers can tell who is publishing and who is reading

Tor encrypts traffic on the local network, and it obscures the eventual destination of the communication, but it doesn't do much to obscure the traffic volume. In particular, a user publishing a home video will have a different network fingerprint than a user reading an online news article. Based on our assumption in Section 2 that users who publish material are in more danger, should we work to improve Tor's security in this situation?

In the general case this is an extremely challenging task: effective *end-to-end traffic confirmation attacks* are known where the adversary observes the origin and the destination of traffic and confirms that they are part of the same communication [8, 24]. Related are *website fingerprinting attacks*, where the adversary downloads a few hundred popular websites, makes a set of "fingerprints" for each site, and then observes the target Tor client's traffic to look for a match [4, 21]. But can we do better against a limited adversary who just does coarse-grained sweeps looking for unusually prolific publishers?

One answer is for bridge users to automatically send bursts of padding traffic periodically. (This traffic can be implemented in terms of long-range drop cells, which are already part of the Tor specification.) Of course, convincingly simulating an actual human publishing interesting content is a difficult arms race, but it may be worthwhile to at least start the race. More research remains.

8.3 Anonymity effects from acting as a bridge relay

Against some attacks, relaying traffic for others can improve anonymity. The simplest example is an attacker who owns a small number of Tor servers. He will see a connection from the bridge, but he won't be able to know whether the connection originated there or was relayed from somebody else. More generally, the mere uncertainty of whether the traffic originated from that user may be helpful.

There are some cases where it doesn't seem to help: if an attacker can watch all of the bridge's incoming and outgoing traffic, then it's easy to learn which connections were relayed and which started there. (In this case he still doesn't know the final destinations unless he is watching them too, but in this case bridges are no better off than if they were an ordinary client.)

There are also some potential downsides to running a bridge. First, while we try to make it hard to enumerate all bridges, it's still possible to learn about some of them, and for some people just the fact that they're running one might signal to an attacker that they place a higher value on their anonymity. Second, there are some more esoteric attacks on Tor relays that are not as well-understood or well-tested—for example, an attacker may be able to "observe" whether the bridge is sending traffic even if he can't actually watch its network, by relaying traffic through it and noticing changes in traffic timing [25]. On the other hand, it may be that limiting the bandwidth the bridge is willing to relay will allow this sort of attacker to determine if it's being used as a bridge but not easily learn whether it is adding traffic of its own.

We also need to examine how entry guards fit in. Entry guards (a small set of nodes that are always used for the first step in a circuit) help protect against certain attacks where the attacker runs a few Tor servers and waits for the user to choose these servers as the beginning and end of her circuit[2]. If the blocked user doesn't use the bridge's entry guards, then the bridge doesn't gain as much cover benefit. On the other hand, what design changes are needed for the blocked user to use the bridge's entry guards without learning what they are (this seems hard), and even if we solve that, do they then need to use the guards' guards and so on down the line?

It is an open research question whether the benefits of running a bridge outweigh the risks. A lot of the decision rests on which attacks the users are most worried about. For most users, we don't think running a bridge relay will be that damaging, and it could help quite a bit.

8.4 Trusting local hardware: Internet cafes and LiveCDs

Assuming that users have their own trusted hardware is not always reasonable.

For Internet cafe Windows computers that let you attach your own USB key, a USB-based Tor image would be smart. There's Torpark, and hopefully there will be more thoroughly analyzed and trustworthy options down the road. Worries remain about hardware or software keyloggers and other spyware, as well as and physical surveillance.

If the system lets you boot from a CD or from a USB key, you can gain a bit more security by bringing a privacy LiveCD with you. (This approach isn't foolproof either of course, since hardware keyloggers and physical surveillance are still a worry).

In fact, LiveCDs are also useful if it's your own hardware, since it's easier to avoid leaving private data and logs scattered around the system.

8.5 The trust chain

Tor's "public key infrastructure" provides a chain of trust to let users verify that they're actually talking to the right servers. There are four pieces to this trust chain.

First, when Tor clients are establishing circuits, at each step they demand that the next Tor server in the path prove knowledge of its private key [11]. This step prevents the first node in the path from just spoofing the rest of the path. Second, the Tor directory authorities provide a signed list of servers along with their public keys—so unless the adversary can control a threshold of directory authorities, he can't trick the Tor client into using other Tor servers. Third, the location and keys of the directory authorities, in turn, is hard-coded in the Tor source code—so as long as the user got a genuine version of Tor, he can know that he is using the genuine Tor network. And last, the source code and other packages are signed with the GPG keys of the Tor developers, so users can confirm that they did in fact download a genuine version of Tor.

In the case of blocked users contacting bridges and bridge directory authorities, the same logic applies in parallel: the blocked users fetch information from both the bridge authorities and the directory authorities for the 'main' Tor network, and they combine this information locally.

How can a user in an oppressed country know that he has the correct key fingerprints for the developers? As with other security systems, it ultimately comes down to human interaction. The keys are signed by dozens of people around the world, and we have to hope that our users have met enough people in the PGP web of trust that they can learn the correct keys. For users that aren't connected to the global security community, though, this question remains a critical weakness.

9 Maintaining reachability

9.1 How many bridge relays should you know about?

The strategies described in Section 7 talked about learning one bridge address at a time. But if most bridges are ordinary Tor users on cable modem or DSL connection, many of them will disappear

[2] http://wiki.noreply.org/noreply/TheOnionRouter/TorFAQ\#EntryGuards

and/or move periodically. How many bridge relays should a blocked user know about so that she is likely to have at least one reachable at any given point? This is already a challenging problem if we only consider natural churn: the best approach is to see what bridges we attract in reality and measure their churn. We may also need to factor in a parameter for how quickly bridges get discovered and blocked by the attacker; we leave this for future work after we have more deployment experience.

A related question is: if the bridge relays change IP addresses periodically, how often does the blocked user need to fetch updates in order to keep from being cut out of the loop?

Once we have more experience and intuition, we should explore technical solutions to this problem too. For example, if the discovery strategies give out k bridge addresses rather than a single bridge address, perhaps we can improve robustness from the user perspective without significantly aiding the adversary. Rather than giving out a new random subset of k addresses at each point, we could bind them together into *bridge families*, so all users that learn about one member of the bridge family are told about the rest as well.

This scheme may also help defend against attacks to map the set of bridges. That is, if all blocked users learn a random subset of bridges, the attacker should learn about a few bridges, monitor the country-level firewall for connections to them, then watch those users to see what other bridges they use, and repeat. By segmenting the bridge address space, we can limit the exposure of other users.

9.2 Cablemodem users don't usually provide important websites

Another attacker we might be concerned about is that the attacker could just block all DSL and cablemodem network addresses, on the theory that they don't run any important services anyway. If most of our bridges are on these networks, this attack could really hurt.

The first answer is to aim to get volunteers both from traditionally "consumer" networks and also from traditionally "producer" networks. Since bridges don't need to be Tor exit nodes, as we improve our usability it seems quite feasible to get a lot of websites helping out.

The second answer (not as practical) would be to encourage more use of consumer networks for popular and useful Internet services.

A related attack we might worry about is based on large countries putting economic pressure on companies that want to expand their business. For example, what happens if Verizon wants to sell services in China, and China pressures Verizon to discourage its users in the free world from running bridges?

9.3 Scanning resistance: making bridges more subtle

If it's trivial to verify that a given address is operating as a bridge, and most bridges run on a predictable port, then it's conceivable our attacker could scan the whole Internet looking for bridges. (In fact, he can just concentrate on scanning likely networks like cablemodem and DSL services—see Section 9.2 above for related attacks.) It would be nice to slow down this attack. It would be even nicer to make it hard to learn whether we're a bridge without first knowing some secret. We call this general property *scanning resistance*, and it goes along with normalizing Tor's TLS handshake and network fingerprint.

We could provide a password to the blocked user, and she (or her Tor client) provides a nonced hash of this password when she connects. We'd need to give her an ID key for the bridge too (in addition to the IP address and port—see Section 6.1), and wait to present the password until we've finished the TLS handshake, else it would look unusual. If Alice can authenticate the bridge before she tries to send her password, we can resist an adversary who pretends to be the bridge and launches a man-in-the-middle attack to learn the password. But even if she can't, we still resist against widespread scanning.

How should the bridge behave if accessed without the correct authorization? Perhaps it should act like an unconfigured HTTPS server ("welcome to the default Apache page"), or maybe it should mirror and act like common websites, or websites randomly chosen from Google.

We might assume that the attacker can recognize HTTPS connections that use self-signed certificates. (This process would be resource-intensive but not out of the realm of possibility.) But even in this case, many popular websites around the Internet use self-signed or just plain broken SSL certificates.

9.4 How to motivate people to run bridge relays

One of the traditional ways to get people to run software that benefits others is to give them motivation to install it themselves. An often suggested approach is to install it as a stunning screensaver so everybody will be pleased to run it. We take a similar approach here, by leveraging the fact that these users are already interested in protecting their own Internet traffic, so they will install and run the software.

Eventually, we may be able to make all Tor users become bridges if they pass their self-reachability tests—the software and installers need more work on usability first, but we're making progress.

In the mean time, we can make a snazzy network graph with Vidalia[3] that emphasizes the connections the bridge user is currently relaying.

9.5 Publicity attracts attention

Many people working on this field want to publicize the existence and extent of censorship concurrently with the deployment of their circumvention software. The easy reason for this two-pronged push is to attract volunteers for running proxies in their systems; but in many cases their main goal is not to focus on actually allowing individuals to circumvent the firewall, but rather to educate the world about the censorship. The media also tries to do its part by broadcasting the existence of each new circumvention system.

But at the same time, this publicity attracts the attention of the censors. We can slow down the arms race by not attracting as much attention, and just spreading by word of mouth. If our goal is to establish a solid social network of bridges and bridge users before the adversary gets involved, does this extra attention work to our disadvantage?

9.6 The Tor website: how to get the software

One of the first censoring attacks against a system like ours is to block the website and make the software itself hard to find. Our system should work well once the user is running an authentic copy of Tor and has found a working bridge, but to get to that point we rely on their individual skills and ingenuity.

Right now, most countries that block access to Tor block only the main website and leave mirrors and the network itself untouched. Falling back on word-of-mouth is always a good last resort, but we should also take steps to make sure it's relatively easy for users to get a copy, such as publicizing the mirrors more and making copies available through other media. We might also mirror the latest version of the software on each bridge, so users who hear about an honest bridge can get a good copy. See Section 7.1 for more discussion.

[3] `http://vidalia-project.net/`

10 Future designs

10.1 Bridges inside the blocked network too

Assuming actually crossing the firewall is the risky part of the operation, can we have some bridge relays inside the blocked area too, and more established users can use them as relays so they don't need to communicate over the firewall directly at all? A simple example here is to make new blocked users into internal bridges also—so they sign up on the bridge authority as part of doing their query, and we give out their addresses rather than (or along with) the external bridge addresses. This design is a lot trickier because it brings in the complexity of whether the internal bridges will remain available, can maintain reachability with the outside world, etc.

More complex future designs involve operating a separate Tor network inside the blocked area, and using *hidden service bridges*—bridges that can be accessed by users of the internal Tor network but whose addresses are not published or findable, even by these users—to get from inside the firewall to the rest of the Internet. But this design requires directory authorities to run inside the blocked area too, and they would be a fine target to take down the network.

11 Next Steps

Technical solutions won't solve the whole censorship problem. After all, the firewalls in places like China are *socially* very successful, even if technologies and tricks exist to get around them. However, having a strong technical solution is still necessary as one important piece of the puzzle.

In this paper, we have shown that Tor provides a great set of building blocks to start from. The next steps are to deploy prototype bridges and bridge authorities, implement some of the proposed discovery strategies, and then observe the system in operation and get more intuition about the actual requirements and adversaries we're up against.

References

1. Alessandro Acquisti, Roger Dingledine, and Paul Syverson. On the economics of anonymity. In Rebecca N. Wright, editor, *Financial Cryptography*. Springer-Verlag, LNCS 2742, 2003.
2. Adam Back, Ian Goldberg, and Adam Shostack. Freedom systems 2.1 security issues and analysis. White paper, Zero Knowledge Systems, Inc., May 2001.
3. Oliver Berthold, Hannes Federrath, and Stefan Köpsell. Web MIXes: A system for anonymous and unobservable Internet access. In H. Federrath, editor, *Designing Privacy Enhancing Technologies: Workshop on Design Issue in Anonymity and Unobservability*. Springer-Verlag, LNCS 2009, 2000.
4. George Dean Bissias, Marc Liberatore, and Brian Neil Levine. Privacy vulnerabilities in encrypted http streams. In *Proceedings of Privacy Enhancing Technologies workshop (PET 2005)*, May 2005. `http://prisms.cs.umass.edu/brian/pubs/bissias.liberatore.pet.2005.pdf`.
5. David Chaum. Blind signatures for untraceable payments. In D. Chaum, R.L. Rivest, and A.T. Sherman, editors, *Advances in Cryptology: Proceedings of Crypto 82*, pages 199–203. Plenum Press, 1983.
6. Ian Clarke, Oskar Sandberg, Brandon Wiley, and Theodore W. Hong. Freenet: A distributed anonymous information storage and retrieval system. In H. Federrath, editor, *Designing Privacy Enhancing Technologies: Workshop on Design Issue in Anonymity and Unobservability*, pages 46–66. Springer-Verlag, LNCS 2009, July 2000.
7. Richard Clayton, Steven J. Murdoch, and Robert N. M. Watson. Ignoring the great firewall of china. In *Proceedings of the Sixth Workshop on Privacy Enhancing Technologies (PET 2006)*, Cambridge, UK, June 2006. Springer. `http://www.cl.cam.ac.uk/~rnc1/ignoring.pdf`.
8. George Danezis. The traffic analysis of continuous-time mixes. In David Martin and Andrei Serjantov, editors, *Privacy Enhancing Technologies (PET 2004)*, LNCS, May 2004. `http://www.cl.cam.ac.uk/users/gd216/cmm2.pdf`.

9. Roger Dingledine and Nick Mathewson. Anonymity loves company: Usability and the network effect. In *Proceedings of the Fifth Workshop on the Economics of Information Security (WEIS 2006)*, Cambridge, UK, June 2006. `http://freehaven.net/doc/wupss04/usability.pdf`.
10. Roger Dingledine, Nick Mathewson, and Paul Syverson. Reputation in P2P Anonymity Systems. In *Proceedings of Workshop on Economics of Peer-to-Peer Systems*, June 2003. `http://freehaven.net/doc/econp2p03/econp2p03.pdf`.
11. Roger Dingledine, Nick Mathewson, and Paul Syverson. Tor: The second-generation onion router. In *Proceedings of the 13th USENIX Security Symposium*, August 2004. `http://tor.eff.org/tor-design.pdf`.
12. Roger Dingledine and Paul Syverson. Reliable MIX Cascade Networks through Reputation. In Matt Blaze, editor, *Financial Cryptography*. Springer-Verlag, LNCS 2357, 2002.
13. Ronald Deibert et al. Psiphon. `http://psiphon.civisec.org/`.
14. Nick Feamster, Magdalena Balazinska, Greg Harfst, Hari Balakrishnan, and David Karger. Infranet: Circumventing web censorship and surveillance. In *Proceedings of the 11th USENIX Security Symposium*, August 2002. `http://nms.lcs.mit.edu/~feamster/papers/usenixsec2002.pdf`.
15. Gina Fisk, Mike Fisk, Christos Papadopoulos, and Joshua Neil. Eliminating steganography in internet traffic with active wardens. In Fabien Petitcolas, editor, *Information Hiding Workshop (IH 2002)*. Springer-Verlag, LNCS 2578, October 2002.
16. Geoffrey Goodell. *Perspective Access Networks*. PhD thesis, Harvard University, July 2006. `http://afs.eecs.harvard.edu/~goodell/thesis.pdf`.
17. Geoffrey Goodell and Paul Syverson. The right place at the right time: The use of network location in authentication and abuse prevention, 2006. Submitted.
18. Bennett Haselton. How to install the Circumventor program. `http://www.peacefire.org/circumventor/simple-circumventor-instructions.%html`.
19. Ip-to-country database. `http://ip-to-country.webhosting.info/`.
20. Stefan Köpsell and Ulf Hilling. How to achieve blocking resistance for existing systems enabling anonymous web surfing. In *Proceedings of the Workshop on Privacy in the Electronic Society (WPES 2004)*, Washington, DC, USA, October 2004. `http://freehaven.net/anonbib/papers/p103-koepsell.pdf`.
21. Brian N. Levine, Michael K. Reiter, Chenxi Wang, and Matthew Wright. Timing analysis in low-latency mix-based systems. In Ari Juels, editor, *Financial Cryptography*. Springer-Verlag, LNCS (forthcoming), 2004.
22. Rebecca MacKinnon. Private communication, 2006.
23. James Marshall. CGIProxy: HTTP/FTP Proxy in a CGI Script. `http://www.jmarshall.com/tools/cgiproxy/`.
24. Nick Mathewson and Roger Dingledine. Practical traffic analysis: Extending and resisting statistical disclosure. In David Martin and Andrei Serjantov, editors, *Privacy Enhancing Technologies (PET 2004)*, LNCS, May 2004. `http://freehaven.net/doc/e2e-traffic/e2e-traffic.pdf`.
25. Steven J. Murdoch and George Danezis. Low-cost traffic analysis of tor. In *IEEE Symposium on Security and Privacy*. IEEE CS, May 2005.
26. Steven J. Murdoch and Stephen Lewis. Embedding covert channels into TCP/IP. In Mauro Barni, Jordi Herrera-Joancomartí, Stefan Katzenbeisser, and Fernando Pérez-González, editors, *Information Hiding: 7th International Workshop*, volume 3727 of *LNCS*, pages 247–261, Barcelona, Catalonia (Spain), June 2005. Springer-Verlag.
27. Thomas H. Ptacek and Timothy N. Newsham. Insertion, evasion, and denial of service: Eluding network intrusion detection. Technical report, Secure Networks, Inc., Suite 330, 1201 5th Street S.W, Calgary, Alberta, Canada, T2R-0Y6, 1998.
28. Ethan Zuckerman. We've got to adjust some of our threat models. `http://www.ethanzuckerman.com/blog/?p=1019`.

Fellowships at the National Endowment for Democracy

Democracy Fellowships

The National Endowment for Democracy (NED) invites applications to its Reagan-Fascell Democracy Fellows Program. Established in 2001 to enable democracy practitioners and scholars from around the world to deepen their understanding of democracy and enhance their ability to promote democratic change, the program is based at NED's International Forum for Democratic Studies, in Washington, D.C.

Program: The program offers five-month fellowships for *practitioners* to improve strategies and techniques for building democracy abroad and five- to ten-month fellowships for *scholars* to conduct original research for publication. *Practitioners* may include activists, lawyers, journalists, and other civil society professionals; *scholars* may include professors, research analysts, and other writers. Projects may focus on the political, social, economic, legal, and cultural aspects of democratic development and may include a range of methodologies and approaches.

Eligibility: The fellows program is intended primarily to support practitioners and scholars *from new and aspiring democracies*. Distinguished scholars from the United States and other established democracies are also eligible to apply. Practitioners are expected to have substantial experience working to promote democracy. Scholars are expected to have a doctorate, or academic equivalent, at the time of application. The program is not designed to pay for professional training or to support students working toward a degree. *A working knowledge of English is an important prerequisite for participation in the program.*

Support: The fellowship year begins October 1 and runs through July 31, with major entry dates in October and March. All fellows receive a monthly stipend, health insurance, travel assistance, and research support through the Forum's Democracy Resource Center and the Reagan-Fascell Research Associates Program.

Application: For further details, please visit us online at **www.ned.org**. For instructions on how to apply, please download our most recent Information and Application Forms Booklet, available at **www.ned.org/forum/R-FApplication.doc** or visit us online at **www.ned.org/forum/reagan-fascell.html.** *All application materials must be type-written and in English.*

Extended Deadline: Applications for fellowships in 2009–2010 must be received no later than **November 10, 2008.** Notification of the competition outcome is in April 2009.

For more information please contact:

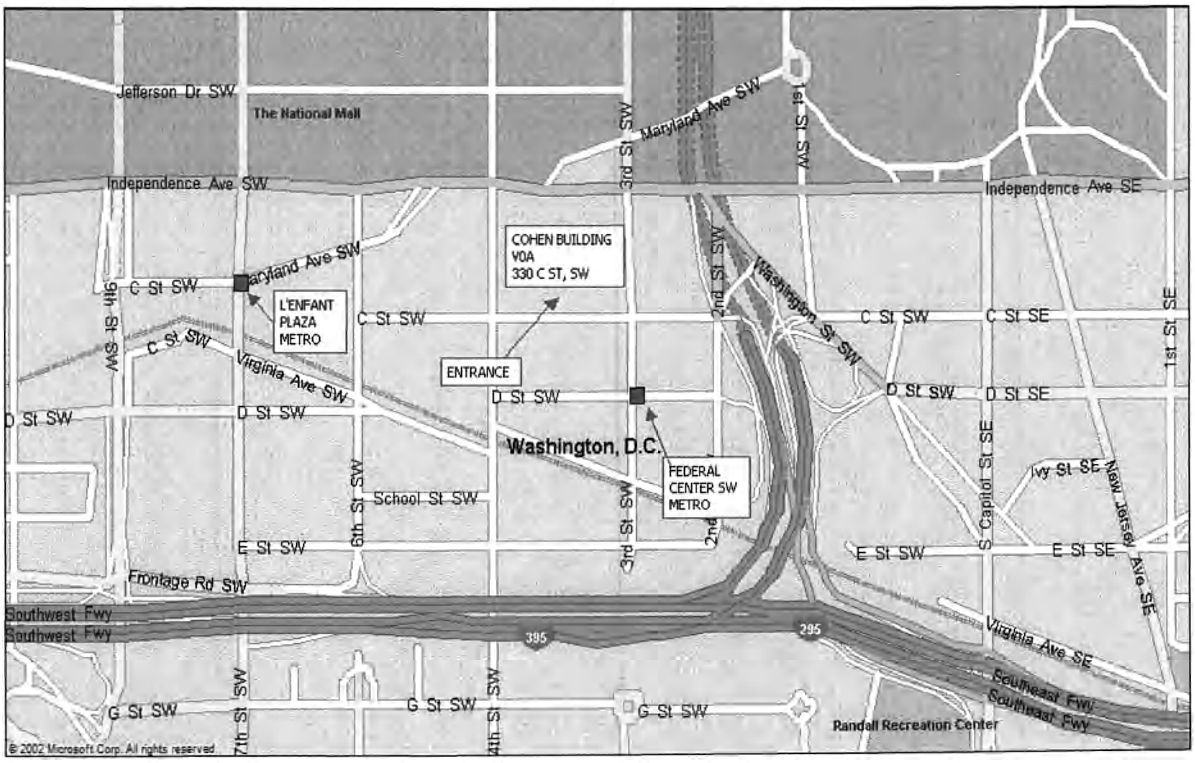
Program Assistant, Fellowship Programs
International Forum for Democratic Studies
National Endowment for Democracy
1025 F Street, N.W., Suite 800
Washington, D.C. 20004

Tel: (202) (b) (6)
Fax: (202) (b) (6)
E-mail: **fellowships@ned.org**
Internet: **www.ned.org**

The International Broadcasting Bureau is in the Cohen Building, kitty-corner to the Air and Space Museum. The formal address is 330 Independence Ave, SouthWest (remember, DC is in four quadrants – don't go to the wrong quadrant!)

The building is bordered by Independence, C Street, 3rd and 4th Streets. The visitor entrance is on C Street. Go in and call my office (b) (6) from the guard's station; if no answer at my desk, call my cell (b) (6)

The closest Metro station is Federal Center SW (Orange & Blue lines), at 3rd and D Street. Walk up one block to C Street and you'll see our building. You can also get off at L'Enfant Plaza station, Maryland Ave exit.



Ken Berman

Esoteric Uses of the Internet

September 20-21, 2006

Hyatt Regency Reston
1800 Presidents Street
Reston, VA

Tuesday, September 19, 2006

7:00 PM	No Host Drinks and Dinner (meet in the Hyatt hotel bar area off of the reception area (***not*** the Market Street Bar and Grill, also in the Hyatt.)

Wednesday, September 20, 2006

8:00-8:30	Registration & Breakfast at Event Facility
8:30-9:00	**Plenary Session** Welcome Opening Brief
9:00-10:00	Consultant Remarks Discussions
10:00-10:15	**Coffee Break**
10:15-11:30	**Plenary Session continues** Consultant Remarks Discussions Instructions for Groups and Breakout Rooms
11:30-12:30	**Lunch**

12:30-2:30	**Group Discussions**
	Groups Report to Breakout Rooms Deliberations & Participation in discussion board
2:30-2:45	**Break**
2:45-4:30	**Group Discussions**
	New focus provided by control or moderators Deliberations & Participation in discussion board
4:30	**Adjourn Day One**
6:00	**No-Host Dinner** – TBA

Thursday, September 21, 2006

8:00-9:00	**Breakfast/ Check Out** (Lodging)
9:00-9:15	**Plenary Session**
9:15-10:15	**Group Discussion wrap up**
	Groups Report to Breakout Rooms
10:15-10:30	**Coffee Break**
10:30-12:30	**Plenary Session**
	Reports by Team Leaders General Discussion Wrap-up
12:30-1:30	**Lunch** Adjourn Day Two
2:00-5:00	Tor Presentations

```
|Time    | client                             |
|        |                | destination       |
|0.000   |       50936 > https [SYN]         |TCP: 50936 > https [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=3
TSV=308243096 TSER=0
|        |(50936) ------------------> (443)  |
|0.541   |       https > 50936 [SYN,         |TCP: https > 50936 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0
MSS=1412 TSV=554740979 TSER=308243096 WS=7
|        |(50936) <------------------ (443)  |
|0.541   |       50936 > https [ACK]         |TCP: 50936 > https [ACK] Seq=1 Ack=1 Win=524280 Len=0
TSV=308243102 TSER=554740979
|        |(50936) ------------------> (443)  |
|0.542   |       Client Hello              |TLSv1: Client Hello
|        |(50936) ------------------> (443)  |
|1.030   |       https > 50936 [ACK]         |TCP: https > 50936 [ACK] Seq=1 Ack=177 Win=6912 Len=0
TSV=554741518 TSER=308243102
|        |(50936) <------------------ (443)  |
|1.033   |       Server Hello,             |TLSv1: Server Hello,
|        |(50936) <------------------ (443)  |
|1.124   |       50936 > https [ACK]         |TCP: 50936 > https [ACK] Seq=177 Ack=1401 Win=523600 Len=0
TSV=308243107 TSER=554741519
|        |(50936) ------------------> (443)  |
|2.079   |       [TCP Previous segme         |TLSv1: [TCP Previous segment lost] Ignored Unknown Record
|        |(50936) <------------------ (443)  |
|2.079   |       [TCP Dup ACK 12#1]           |TCP: [TCP Dup ACK 12#1] 50936 > https [ACK] Seq=177 Ack=1401
Win=523600 Len=0 TSV=308243117 TSER=554741519 SLE=4201 SRE=4682
|        |(50936) ------------------> (443)  |
|5.563   |       [TCP Retransmission         |TCP: [TCP Retransmission] [TCP segment of a reassembled PDU]
|        |(50936) <------------------ (443)  |
|5.563   |       50936 > https [ACK]         |TCP: 50936 > https [ACK] Seq=177 Ack=2801 Win=522200 Len=0
TSV=308243152 TSER=554746089 SLE=4201 SRE=4682
|        |(50936) ------------------> (443)  |
|6.008   |       [TCP Retransmission         |TLSv1: [TCP Retransmission] Ignored Unknown Record
|        |(50936) <------------------ (443)  |
|6.008   |       50936 > https [ACK]         |TCP: 50936 > https [ACK] Seq=177 Ack=4682 Win=523112 Len=0
TSV=308243156 TSER=554746545
|        |(50936) ------------------> (443)  |
|16.025  |       Client Key Exchange         |TLSv1: Client Key Exchange, Change Cipher Spec, Encrypted Handshake
Message
|        |(50936) ------------------> (443)  |
|17.533  |       [TCP Retransmission         |TLSv1: [TCP Retransmission] Client Key Exchange, Change Cipher Spec,
Encrypted Handshake Message
|        |(50936) ------------------> (443)  |
|20.735  |       [TCP Retransmission         |TLSv1: [TCP Retransmission] Client Key Exchange, Change Cipher Spec,
Encrypted Handshake Message
|        |(50936) ------------------> (443)  |
|21.127  |       [TCP Previous segme         |TCP: [TCP Previous segment lost] https > 50936 [ACK] Seq=4741
Ack=375 Win=7936 Len=0 TSV=554761712 TSER=308243303 SLE=177 SRE=375
|        |(50936) <------------------ (443)  |
|26.447  |       50936 > https [FIN,         |TCP: 50936 > https [FIN, ACK] Seq=375 Ack=4682 Win=524280 Len=0
TSV=308243361 TSER=554746545
|        |(50936) ------------------> (443)  |
|26.743  |       Encrypted Alert           |TLSv1: Encrypted Alert
|        |(50936) <------------------ (443)  |
|26.743  |       50936 > https [RST]         |TCP: 50936 > https [RST] Seq=376 Win=0 Len=0
|        |(50936)  ------------------>  (443)  |
```

The Tor Project
969 Main Street, #206
Walpole, MA 02081

Statement

Date
12/31/2011

To:
IBB-Contract 2

Amount Due	Amount Enc.
$45,000.00	

Date	Transaction	Amount	Balance
12/31/2010	Balance forward		30,000.00
01/11/2011	DEP Inv #31	-15,000.00	15,000.00
01/31/2011	INV #Int # 33.	15,000.00	30,000.00
02/28/2011	INV #IBB #34.	15,000.00	45,000.00
03/03/2011	DEP Inv #33	-15,000.00	30,000.00
03/31/2011	INV #IBB #35.	15,000.00	45,000.00
04/11/2011	DEP Inv 34	-15,000.00	30,000.00
04/30/2011	INV #IBB #36.	15,000.00	45,000.00
05/05/2011	DEP 04082011 inv	-15,000.00	30,000.00
05/31/2011	INV #IBB #37.	15,000.00	45,000.00
06/13/2011	DEP Inv 36	-15,000.00	30,000.00
06/30/2011	INV #IBB #38.	15,000.00	45,000.00
07/12/2011	DEP Inv 37	-15,000.00	30,000.00
07/31/2011	INV #IBB # 39.	15,000.00	45,000.00
08/31/2011	INV #IBB # 40.	15,000.00	60,000.00
09/08/2011	DEP Inv 39	-15,000.00	45,000.00
09/30/2011	INV #IBB #41.	15,000.00	60,000.00
10/13/2011	DEP	-15,000.00	45,000.00
10/31/2011	INV #IBB# 42.	15,000.00	60,000.00
11/15/2011	DEP For inv #41	-15,000.00	45,000.00

CURRENT	1-30 DAYS PAST DUE	31-60 DAYS PAST DUE	61-90 DAYS PAST DUE	OVER 90 DAYS PAST DUE	Amount Due
0.00	0.00	0.00	15,000.00	30,000.00	$45,000.00

Building Incentives into Tor

Author names removed for anonymous submission

Abstract

Distributed anonymous communication networks depend on volunteers to donate their resources. In the case of Tor, one of the most popular and widely used anonymity systems, the efforts of volunteers have not grown as fast as the demands on Tor. This disparity is limiting its performance. In this paper, we explore techniques to incentivize Tor users to establish Tor relays; if a user contributes resources to the Tor overlay, they should receive faster service in return. We propose a design where the central Tor directory authorities measure performance and publish a list of Tor relays that should be given higher priority when establishing circuits. We implemented and evaluated event-driven simulations of our proposed design, showing that conforming nodes receive significant improvements in performance, in some cases experiencing twice the network throughput of selfish users who do not relay traffic for the Tor network. Our system provides an acceptable anonymity tradeoff and improves performance while incentivizing Tor users, across the whole network, to contribute the resources necessary for Tor to better support its users' needs.

I. Introduction

Anonymizing networks such as Tor [16] and Mixminion [12] aim to provide protection from traffic analysis on the Internet. While encryption focuses on the content of communication, traffic analysis focuses on who is communicating with whom, which users are using which websites, and so on. These anonymity systems have a broad range of users, including ordinary citizens who want to avoid being profiled for targeted advertisements, corporations who do not want to reveal information to their competitors, and law enforcement and government intelligence agencies who need to interact with the Internet without being noticed.

These networks work by bouncing traffic around a network of relays operated around the world, and strong security comes from having a large and diverse network. To this end, Tor has built a community of volunteer relay operators. This approach can provide sustainability (the network doesn't shut down when the money runs out) and diversity (many different groups run relays for many different reasons), but it can also be a weakness if too few people choose to operate relays to support the network's traffic.

In fact, Tor is heading in exactly this direction. The number of users keeps growing, while a variety of factors discourage more people from setting up relays; some want to save their bandwidth for their own use, some can't be bothered to configure port forwarding on their firewall, and some worry about the possible consequences from running a relay. This growing user-to-relay ratio in turn hurts the service received by all users, leading to a classic "tragedy of the commons" situation [24].

Worse, not all users are equal; while Tor was designed for web browsing, instant messaging, and other low-bandwidth communication, an increasing number of Internet users are looking for ways to anonymize high-volume communications. We did an informal measurement study by running a Tor exit relay at our institution, and we found that the median connection coming out of our relay looked like HTTP traffic, but the median *byte* looked like file-sharing traffic.

The Tor designers argued in 2005 [17] that having too much load on the Tor network should be self-correcting, since low bandwidth and poor performance would drive away users until the users that remain have acceptable performance. But the current Tor network does not match their prediction. We suggest this disparity is because different activities have different tolerance for bad performance: users of interactive applications like web browsing give up before the file-sharers, who are less sensitive to waiting hours for their work to complete.

How can we get more people to run relays for Tor? There are three common approaches to encouraging people to offer service in the p2p world: building community, making it easier to run relays, and providing improved performance in exchange for service. So far Tor has focused most on the first approach. By attracting people who believe strongly in anonymous communications to run relays, and building a community where relay operators are respected and appreciated, Tor has grown to become the largest anonymity network ever; at this point there are over 1000 relays pushing over 1GBit/s of aggregate traffic. To make it easier to run relays, Tor includes features like rate limiting and exit policies, and we describe in Section VIII some additional features we have helped them add to further lower the barrier of setting up a relay.

However, the third approach (giving better performance for users who relay) has always been considered tricky, since tracking users and keeping statistics can introduce new anonymity attacks. After all, these networks are specifically designed to make it hard to identify the origin of a connection, so any sort of accounting scheme seems to be at odds with preserving anonymity.

In this paper, we propose a solution for Tor where the central directory authorities measure the performance of individual relays and use this information to construct a list of well-behaving relays. Relays obtain this list from the directory authorities during normal updates. To allow relays to be treated differently, traffic from relays in the list is marked as high priority by other relays and receives better treatment along the whole circuit. We show through simulation that this design can improve the performance for listed relays, even as traffic from other users increases. This approach incentivizes end users to establish new Tor relays, improving Tor for everybody. There are some anonymity implications from our new design, the most notable of which is that we end up with two anonymity sets: the group of well-behaving relays and the group of other users and relays. We argue that the new design provides an acceptable tradeoff between improved performance and decreased potential for anonymity.

The rest of the paper is organized as follows. Section II provides background on Tor. Section III investigates exactly which behaviors we need to incentivize. Section IV describes our proposed design and Section V presents its simulation results. We discuss the results in Section VI, and review related works in Section VII. We examine how to integrate our changes into Tor's design in Section VIII, and Section IX concludes.

II. Background

A. Tor design

The Tor network is an overlay network of volunteers running *Tor relays* that relay TCP streams for *Tor clients*. Tor aims to let its users connect to Internet destinations like websites while making it hard for 1) an attacker on the client side to learn the intended destination, 2) an attacker on the destination side to learn the client's location, and 3) any small group of relays to link the client to her destinations.

To connect to a destination website or other service via Tor, the client software incrementally creates a private pathway or *circuit* of encrypted connections through several Tor relays, negotiating a separate set of encryption keys for each hop along the circuit. The circuit is extended one hop at a time, and each relay along the way knows only the immediately previous and following relay in the circuit, so no single Tor relay knows the complete path that each fixed-sized data packet (or *cell*) will take. Thus, neither an eavesdropper nor a compromised relay can see both the connection's source and destination. Clients periodically rotate to a new circuit, to complicate long-term linkability between different actions by a single user.

The client learns which relays it can use by fetching a signed list of Tor relays from one of the *directory authorities*. Each authority lists the available relays along with a set of opinions or recommendations for each: whether the authority believes the relay to be reliable, fast, and so on. Clients make their decisions based on the majority consensus of authority opinions; each authority's signing key comes with the Tor software so clients can know they are starting with the right information.

More specifically, Tor's directory authorities play three roles. First, they provide a trust root so Tor clients can't be tricked into using an alternate network run by an attacker. Second, they track which relays are available and reliable so each user doesn't have to independently discover this information. Last, they provide a way for Tor users to synchronize their behavior; since anonymity loves company, users that make decisions based on similar information will blend together better [15]. Directory information is cached on most Tor relays, so while the directory authorities are still a trust bottleneck, in practice they're not a performance bottleneck.

To encourage the network to grow, Tor relays have a lot of flexibility. Each relay can rate limit the traffic it relays. To support users with bandwidth caps, relays can specify a maximum amount of traffic to relay in a given period. Further, each relay has its own *exit policy* that specifies to what addresses and ports outside the network it is willing to connect. (Some relays act as non-exit nodes and just relay traffic within the network, some use the default exit policy which disallows a few particularly abuse-prone or bandwidth-heavy ports, and some configure their own custom policy.) Each relay periodically publishes to the directory authorities a self-signed *descriptor* that includes its address, keys, rate limiting information, estimated bandwidth capacity, and exit policy. A more detailed description of the Tor design can be found in its original design document [16] and its specifications [14].

B. Design tradeoffs

Anonymity designs can be divided into two groups based on their goals: *high-latency* and *low-latency*. High-latency designs like Mixmaster [31] and Mixminion [12] can take hours to deliver messages, but because messages mix with each other they can withstand quite powerful attackers. These designs are most suitable for latency-tolerant applications like email, but it turns out the number of people willing to use such networks is small, and this small anonymity set in turn limits the anonymity they can achieve in practice [15].

On the other hand, low-latency designs are more usable for interactive communications like web browsing and instant messaging. While many theoretical anonymity designs demand precise synchronization between all users and incredible bandwidth overhead (e.g., Pipenet [10] and DC-nets [6]), Tor instead chooses to build a practical and useful network and try to achieve good security within these constraints. To that end, Tor doesn't batch or reorder messages at each hop. This choice means that Tor circuits are vulnerable to *end-to-end correlation attacks*: an attacker who can measure traffic at both ends of the circuit can link them [11], [28].

A variety of other anonymity-breaking attacks become possible because of Tor's requirement to remain useful for low-latency communications [26], [29], [32], [33], [38], [40]. Because Tor aims to resist *traffic analysis* attacks (attacks that try to pick the communicants out of a large set of participants) but does not aim to protect against correlation attacks (attacks that watch two suspected endpoints to confirm the link), we have some flexibility in what design changes we can propose. As long as we don't introduce any attacks that are worse than the correlation attacks, we are still within Tor's threat model.

C. Context: the current Tor network

While we haven't yet performed a comprehensive measurement study, we gathered some informal statistics that can give us better intuition about what problems need to be solved. In particular, we investigated the overall set of current Tor users, and we looked at current network usage.

Estimating the number of Tor users is tricky; after all, Tor is an anonymity system. But while Tor aims to prevent attackers from learning what destinations a user visits, it doesn't try to hide which people are *using* Tor. We ran a directory cache long enough to be considered stable and high-bandwidth, and then observed 100492 distinct IP addresses make directory requests over the 24 hour period starting at 10am on Oct 23, 2007. Using the ip2country GeoIP database, we found that roughly 60% of the IP addresses were evenly divided between the United States, Germany, and China, and the rest were spread over 143 other country-codes. While we probably over-counted users with dynamic IP addresses, and we probably under-counted users because we only measured one of the several hundred directory caches, this gives us a ballpark estimate showing that the number of users far exceeds the number of available relays.

We also looked at current network usage by running a Tor relay and recorded summary statistics about its exit traffic over a four-day period starting at 1pm on Mar 13, 2006. Among all the exit connections initiated by Tor users, over 75% are to port 80. Also, over 80% of the connections lasted for less than ten seconds. Moreover, over 97% of the connections sent at most three cells, yet the inbound traffic contains more cells and follows a heavy-tailed distribution. All these hint the most frequent use case for Tor is something similar to web traffic [9]. On the other hand, even though port 80 is the mostly used port, it only accounts for around 1/4 of the total bandwidth, and no other port consumes more than 4% of the total bandwidth. This means there is a small number of connections, using different port numbers, consuming most of the bandwidth. We believe these are sharing and/or downloading large files using common protocols like BitTorrent, and we expect the issue to become worse over time.

Because of the threat of legal actions from the entertainment industry, some users of peer-to-peer file-sharing applications are starting to tunnel their traffic through Tor. In fact, the Azureus BitTorrent client, one of the most popular BitTorrent clients, has built-in support for using Tor. Even though the default Tor exit policy rejects the default BitTorrent ports, enough users are using non-standard ports for their file-sharing that this additional load on an already overloaded network makes the service bad for all users.

III. Incentive Goals

Relayed traffic is traffic forwarded from a Tor client or Tor relay to another relay within the network. Choosing to relay traffic can provide better anonymity in some cases: an attacker who controls the user's next hop would not be able to know whether the connection originated at the user or was relayed from somebody else. But the exact details of the potential anonymity improvement are not well-understood even by the research community. Therefore they are hard to communicate to users, so any potential perceived gains do not outweigh the costs of setting up relaying and providing bandwidth to others.

Tor relays may also opt to serve as exit relays. *Exit traffic* is traffic forwarded from a relay in the Tor network to somewhere outside the network, as well as return traffic from outside back into the network. While there are theoretical anonymity improvements similar to those for relaying traffic, as well as potential legal advantages for the relay operator from not necessarily being the originator of all traffic coming from the relay's IP address [20], in practice the destination website and the user's ISP have no idea that Tor exists, and so they assume all connections are from the operator. Some ISPs tolerate abuse complaints better than others. This hassle and legal uncertainty may drive users away from running as an exit relay.

Beyond creating incentives to relay traffic inside the Tor network and to allow connections to external services, we also need to consider the *quality* of the traffic (e.g., the latency and throughput provided, and the reliability and consistency of these properties). Since Tor circuits pass over several relays, the slowest relay in the circuit has the largest impact.

Depending on the demands facing the Tor network at any given time, we may want to incentivize nodes to both relay traffic at a given quality level and to support exit traffic. Just as we might determine whether a node is properly relaying traffic, we can likewise determine whether a node is properly handling exit traffic. We would then only need to publish the desired policy; users desiring higher priority for their traffic would then decide whether to follow the policy. As such, while the design and analysis in this paper will largely focus on incentivizing relay traffic, other policies and extensions would be straightforward to implement if they became necessary.

IV. Design

Our goal is to encourage users to act as high-quality Tor relays. In this section, we describe our proposed design.

A. Design alternatives

While rewarding good relays with better service sounds simple, implementing it on a system like Tor is not easy. How can one make decisions on who should get priority, when traffic is passed through an anonymizing network? If we rely on Tor users to report their experience, they could indirectly reveal the circuits they used, aiding attacks on anonymity. If we ask the relays to report their experience, they might strategically lie about the results, or they might reveal information that could violate users' anonymity. Any use of "hearsay" evidence that cannot be validated is an opportunity for fraud. If saying good things about a peer can increase its reputation, then we now have an incentive for Sybil attacks [19], creating an army of nodes whose purpose is to speak admiringly of a given node to improve its reputation.

Instead, since Tor already has globally trusted directory authorities, we can extend their role to directly perform measurements and publish the results. The other option is for nodes to directly measure their peers' performance in a fashion analogous to the tit-for-tat trading strategies used in BitTorrent [7] or the peer auditing in Scrivener [34].

a) Central vs. distributed measurement: If we perform centralized measurements, then peers need not have any trust in one another. Likewise, the system will respond quickly when the central authority publishes a finding. Best of all, none of the published information would compromise the anonymity of other Tor traffic. The only information ever measured or published is whether a given node passed an audit for properly relaying its traffic.

Scrivener, for contrast, uses no central authorities, and instead relies on nodes publishing their relative bandwidth debts and credits, which are then used to identify paths in the "debt space." These debt paths are an essential way to overcome the otherwise limited direct relationships that may be observed between nodes. Publishing data like this would be devastating for anonymity as it would allow observers to piece together Tor's data circuits, piece by piece, by observing the bandwidth debts changing in synchrony from one relay node to the next. If each node kept its observations strictly to itself (as with BitTorrent's tit-for-tat measurements), then a given relay node would only be aware of a few peers' current behavior. Stale or absent knowledge of remote peers' behavior might then lead to incorrect decisions on whether to prioritize those nodes' traffic. It might also lead to *partitioning attacks* [12]; when users aren't all acting on the same information and being given the same treatment, an observer may be able to distinguish one user from others. An active attacker can even manipulate network views to induce these attacks.

The only downside of centralized measurement is that it becomes a central point of failure. Tor actually has a number of directory authorities run by disjoint entities who do not necessarily trust one another. In principle, any of these nodes, or any other third party, could act as a measurement authority. The only inescapable requirement is having a centrally trusted authority endorse the measurement authorities. These trade-offs seem manageable, so we will pursue this "centralized" architecture.

b) Other alternatives: A wide variety of creative alternatives might also be possible. We could imagine, for example, using an anonymous digital cash scheme where relays earn cash for relaying traffic from users, but there are still traffic analysis attacks when users go to the bank to deposit or withdraw coins (these attacks may be done by an observer or also by a colluding bank). We would also need a secondary protocol for resolving disputes when one side fails to hold up its end of the bargain. Another alternative might be to leverage social networks' trust relationships, which have been used in a variety of past p2p systems to improve robustness (see, e.g., Sprout [30] and SybilGuard [45]). Unfortunately, if any reputation system included a mechanism for relays to determine that they are friends with the originator of the circuit, those mechanisms could be leveraged to attack users' anonymity. Using reputation systems without compromising anonymity may be possible, but it would be difficult to do properly.

B. Detailed solution

Above, we focused largely on how to *measure* whether a node is behaving correctly. Now we show how to use these measurements to construct a system that incentivizes correct system behavior. Only a tiny fraction of Tor clients currently operate as relays. Therefore, a straightforward incentive scheme would be to provide cooperative users better service by giving their connections priority treatment. However, the very nature of anonymizing network prevents exactly that; when a relay receives a cell, it should not be able to tell which user originated this cell. Thus we must consider less direct reward schemes.

First, note that to provide proper treatment for traffic from different relays, an intermediate relay does not need to know the identity of the origin; in fact, it suffices for the relay to only know the priority of the cell. Our problem now reduces to how the intermediate relay can reliably obtain this information. If it relies on the predecessor relay, a selfish relay could always claim its own traffic as high priority and enjoy the benefit.

Our solution for this problem is to give "gold star" status to relays that provide good service to others. A gold star relay's traffic is given high priority by other relays. This priority treatment is transitive. In other words, when a gold star relay receives high priority from another gold star relay, it labels its outbound traffic as such, and it remains high priority when it forwards to the next relay. All other traffic gets low priority. If a low priority node relays data through a gold star relay, the outbound circuit will not pass along the gold star, and thus the low priority node cannot gain the higher priority given to gold star traffic.

As discussed above, we can leverage Tor's existing directory authorities to actively measure the performance of each individual relay and only grant those with satisfactory performance the gold star status. This measurement can include bandwidth and latency of the relayed traffic for that relay. By measuring the bandwidth through the Tor network itself, the directory authorities can hide their identity and intent from the Tor relays. This method of anonymously auditing nodes' behavior is similarly used in other systems [18], [35], [41].

Due to variations of the network conditions and the multi-hop nature of Tor, it may take multiple measurements to get accurate results. Therefore, we use a "k out of n" approach, where a relay has to have satisfactory performance for k times out of the last n measurements to be eligible for gold star status. Out of all eligible relays, only the top $7/8$ of them are then given the gold star. This is similar to the current Tor design, where the bottom one-eighth of Tor relays (ordered by speed) are not used to relay traffic. The directory authorities can then make the gold star status available through the normal means of distributing relay information.

The effectiveness of this approach depends on the accuracy of the measurements which in turn depends on the measurement frequency. Frequent measurements increase our confidence, but they also place an increasing burden on the overlay network and limit the scalability of the measuring nodes.

Of course, this two-level status classification is very coarse. For instance, it does not differentiate a very fast relay from a moderately fast relay. However, we prefer not to make the classifications any finer, as any such information could potentially be abused by an adversary for deanonymizing the traffic by monitoring traffic priorities.

V. Experiments

In this section, we show simulation results of Tor networks under different scenarios. Our goal is to evaluate the effectiveness of our "gold star" incentive scheme against a variety of different scenarios, including varying amounts of load on the Tor network, and varying strategies taken by simulated nodes (e.g., selfish vs. cooperative).

A. Experimental apparatus

We built a packet-level discrete event simulator that models a Tor overlay network. The simulator is written in Java and was executed on 64-bit AMD Opteron 252 dual core servers with 4GB of RAM and running RedHat Enterprise Linux (kernel version 2.6.9) and Sun's JVM, version 1.5.0.

We simulate every cell at every hop. Each node, particularly simulated BitTorrent clients, can easily have hundreds of outstanding cells in the network at any particular time. Unsurprisingly, the simulations are slow and memory-intensive. In fact, in some larger scale simulations, the simulated time is slower than the wall clock time. Likewise, memory usage is remarkable. Simulating 20 BitTorrent clients and 2000 web clients consumes most of the available memory. To keep the client-to-relay ratio realistic, we could only simulate Tor networks with around 150 relays.

For simplicity, we assumed the upstream and downstream bandwidth for all relays is symmetric, since the forwarding rate of any relay with asymmetric bandwidth will be limited by its lower upstream throughput. We also simplify relays by assuming they take no processing time. The cooperative relays (which reflect the altruists in the current Tor network) have a bandwidth of 500KB/s. The latency between any two nodes in the network is assumed to be fixed at 100 ms.

Our simulations use different numbers of simplified web and BitTorrent clients to generate background traffic. Our web traffic is based on Hernández-Campos et al. [25]'s "Data Set 4," collected in April 2003 [42]. Our simplified BitTorrent clients always maintain four connections and will upload and download data at the maximum speed Tor allows. They also periodically replace their slowest connection with a new one, much like the real BitTorrent seeks to maximize the download rate from its available connections. We assume that the external web or BitTorrent servers have unlimited bandwidth. The different relay traffic types are:

Cooperative These nodes will use their entire 500KB/s bandwidth to satisfy the needs of their peers, and will give priority to "gold star" traffic when present. (If sufficient Gold Star traffic is available to fill the entire pipe, regular traffic will be completely starved for service.)

Selfish These nodes *never* relay traffic for others. They are freeloaders on the Tor system with 500KB/s of bandwidth.

Cooperative slow These nodes follow the same policy as cooperative nodes, but with only 50KB/s of bandwidth.

Cooperative reserve These nodes have 500KB/s bandwidth, just like cooperative nodes, but cap their relaying at 50KB/s, unless they are currently using a connection for their own traffic, in which case they do not cap that connection.

Adaptive These nodes will behave just like cooperative nodes until they get a gold star. After this, they will change to the selfish policy until they lose the gold star.

All of our simulations use ten directory authorities. To assign the gold star status, every minute each directory authority will randomly build a circuit with three Tor relays and measure its bandwidth by downloading a small 40KB file from an external server. The bandwidth measurement is recorded and attributed to only the middle relay in the circuit. (In a genuine deployment, the entry and exit nodes would be able to determine that they were being measured by virtue of being connected to known measurement nodes and could thus change their behavior in response; see Section VI-A for more discussion.) To obtain a gold star, we require Tor relays to successfully relay traffic at least two times out of the last five measurements (i.e., $k = 2$ and $n = 5$ in Section IV-B).

When we report our simulation results, we will describe the observed network performance in terms of "download time" and "ping time." The former describes the necessary time for each node to download a 100KB file from an external server. The latter describes the round-trip latency for that same external server. (For our simulations, this external server is assumed to have infinite bandwidth and introduce zero latency of its own.) Both measures are important indicators of how a Tor user might perceive the quality of the experience when web surfing. For contrast, a Tor user running file-sharing software or downloading large files will be largely insensitive to latency.

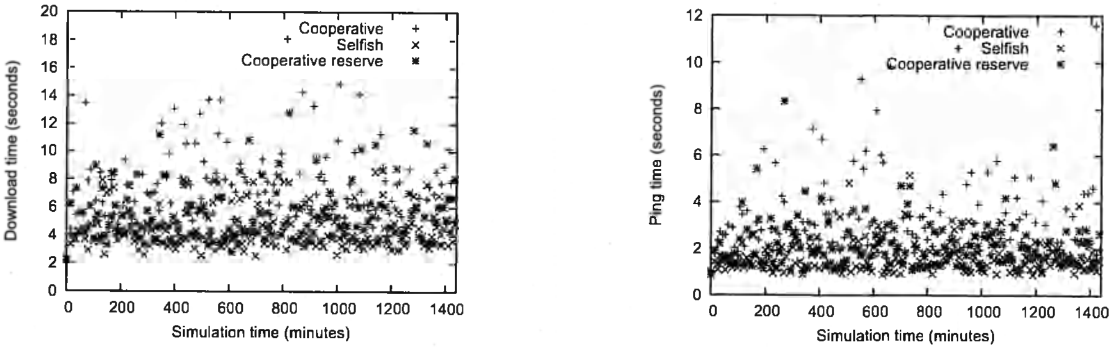


Fig. 1. Average download and ping time over time when no incentive scheme is in place and heavy traffic (20 BitTorrent clients and 2000 web clients). Both download and ping time show significant variation, regardless of relay type.

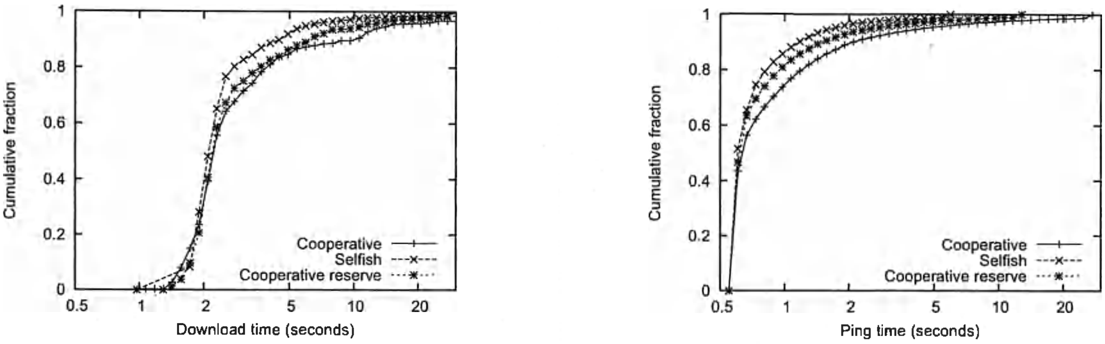


Fig. 2. Cumulative download and ping time when no incentive scheme is in place and heavy traffic (20 BitTorrent clients and 2000 web clients). Performance for all relay types is similar, although selfish relays do somewhat better in the worst case.

B. Experiment 1: Unincentivized Tor

First, we want to understand how Tor networks behave when demand for the network's resources exceeds its supply. In this experiment, we simulate 50 cooperative relays, 50 selfish relays, and 50 cooperative reserve relays, with heavy background traffic (20 BitTorrent clients and 2000 web clients).

Figure 1 plots the *average* download and ping time for each relay type. Even after averaging for 50 relays, the data points are still highly fluctuating, suggesting that the network performance is variable (and appears to be a long-tailed distribution). This is largely due to the BitTorrent traffic, as it sometimes dominates the available bandwidth, starving other circuits sharing the same relays for bandwidth.

To get a better view of the distribution of download times and ping times, we use cumulative distribution functions (CDFs). Figure 2 represents the same data as Figure 1, albeit without any of the averaging. The x-axis represents download time or ping time and the y-axis represents the percentage of nodes who experienced that particular download or ping time *or less*.

While the ideal download time for all relay types in this experiment is 0.8 second (six network roundtrip hops plus bandwidth time), all relay types rarely achieve anywhere close to this number. Figure 2 clearly shows that roughly 80% of the attempted downloads take more than two seconds, regardless of a node's policy. Cooperative relays have approximately 10% taking longer than ten seconds. Less than 5% of the selfish nodes see performance this bad. Selfish nodes, in general, do better in the worst case than cooperative nodes, but observe similar common-case performance.

C. Experiment 2: Gold Stars

Our first experiment represents the present-day situation in the Tor network and is clearly unsatisfactory. This experiment measures the effectiveness of our "gold star" mechanism in addressing this concern. This time, our simulation consists of 40 cooperative relays, 40 selfish relays, 40 cooperative slow relays, and 40 adaptive relays. These variations, relative to the first experiment, also allow us to see whether slower cooperative nodes still get the

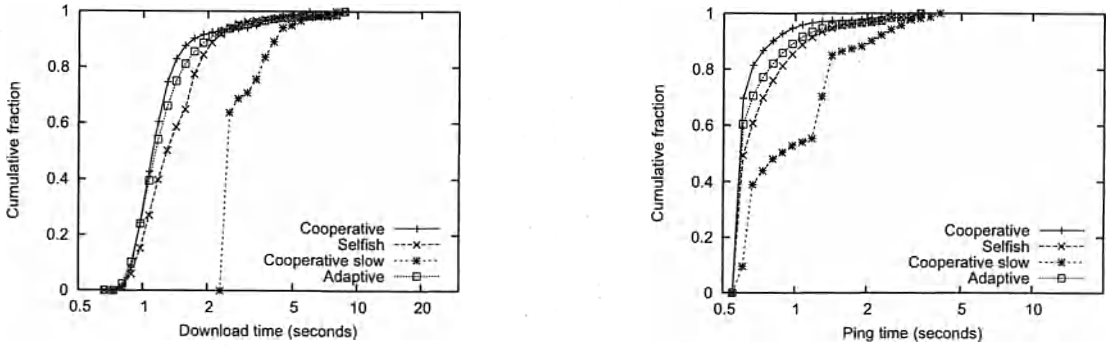


Fig. 3. Cumulative download and ping time with the gold star scheme and no background traffic.

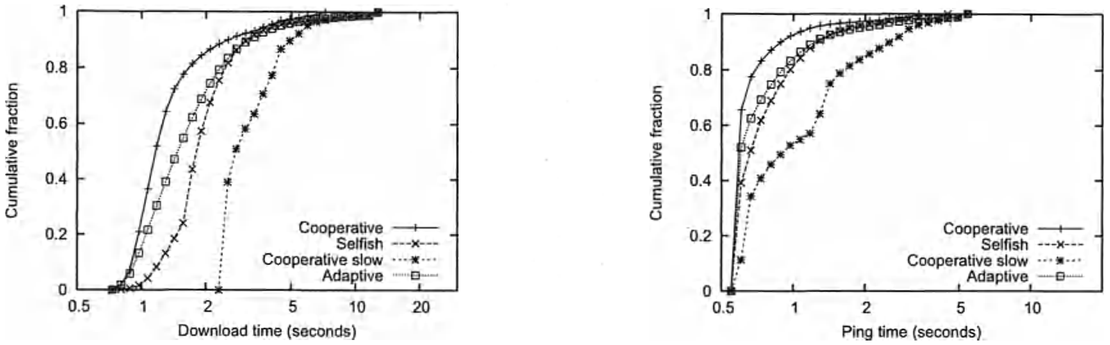


Fig. 4. Cumulative download and ping time with the gold star scheme and light background traffic (10 BitTorrent clients and 1000 web clients). Selfish and adaptive relays now begin to suffer while cooperative relays maintain their performance.

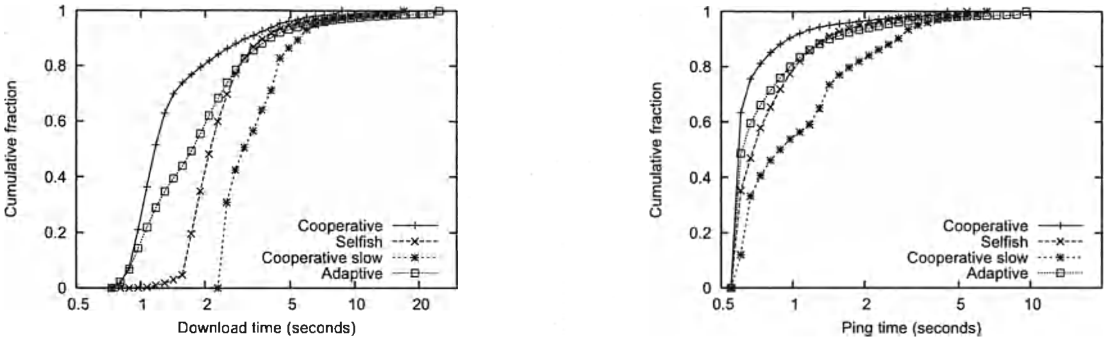


Fig. 5. Cumulative download and ping time with the gold star scheme and heavy background traffic (20 BitTorrent clients and 2000 web clients). Cooperative nodes maintain their performance, while the penalty for selfish and adaptive nodes is more pronounced.

benefits of a gold star, and whether adaptive nodes can be more effective than purely selfish nodes. Figures 3, 4, and 5 show the cumulative download and ping time with no background traffic, light background traffic, and heavy background traffic, respectively.

Our results are striking. Cooperative nodes maintain their performance, regardless of the level of background traffic in the overlay. When there is no background traffic, they slightly outperform the selfish and adaptive nodes, but once the traffic grows, the cooperative nodes see clear improvements in download time and in latency. For example, under heavy background traffic, 80% of the cooperative nodes see download times under two seconds, versus roughly 2.5 seconds for the selfish and adaptive nodes.

Our experiment shows that the adaptive policy is ineffective at defeating the gold star mechanism. Adaptive nodes will experience better performance while they have a gold star, but their benefit only splits the difference between the cooperative and selfish policies, roughly in proportion to the additional effort they are spending to maintain their gold star.

Cooperative slow nodes, like their fast counterparts, experience stable performance as the background load on the

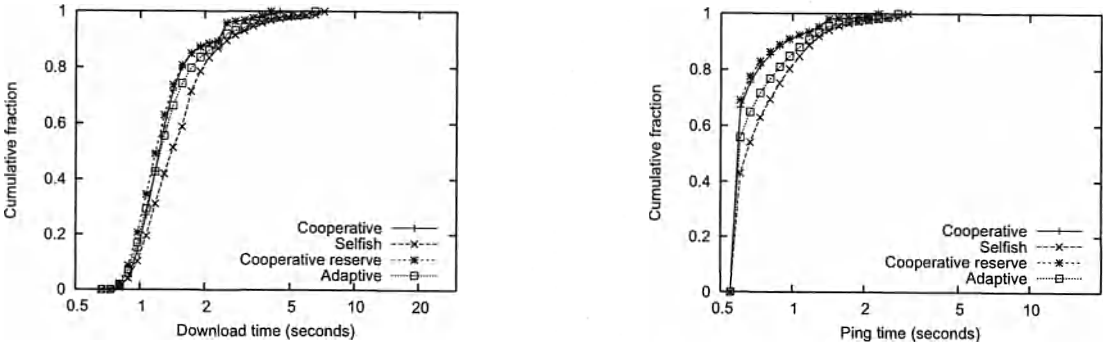


Fig. 6. Cumulative download and ping time with gold star scheme and no background traffic. Cooperative reserve relays, which replaced cooperative slow relays, have similar performance with cooperative relays.

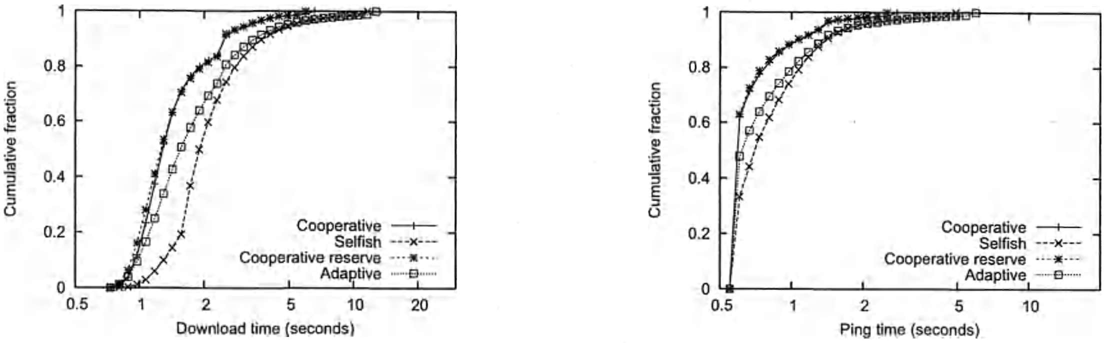


Fig. 7. Cumulative download and ping time with gold star scheme and light background traffic (10 BitTorrent clients and 1000 web clients). Only selfish and adaptive relays are affected with the increased traffic.

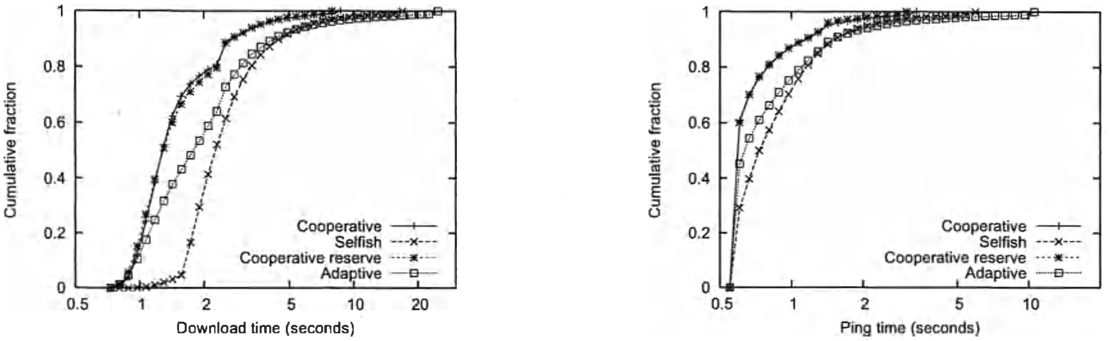


Fig. 8. Cumulative download and ping time with gold star scheme and heavy background traffic (20 BitTorrent clients and 2000 web clients). Again, cooperative and cooperative reserve relays are not affected, while the performance of selfish and adaptive relays become much worse.

Tor network increases. This demonstrates that the gold star policy can effectively reward good behavior, regardless of a node's available bandwidth.

We conducted a further experiment, replacing the cooperative slow nodes with cooperative reserve nodes, representing a possibly rational response to the gold star mechanism. As a node only needs to prove that it is relaying data in order to get the gold star, then it might benefit by reserving most of its bandwidth for its own needs, here using only 10% of its bandwidth for its contributions to the good of other nodes. Figures 6–8 show the results of this experiment.

In each condition, both kinds of cooperative nodes observe identical distributions of bandwidth and latency. Again, selfish and adaptive nodes suffer as the background traffic increases. This experiment shows, unsurprisingly, that nodes need not be "fully" cooperative to gain a gold star. In an actual Tor deployment, it would become a policy matter, perhaps an adaptive process based on measuring the Tor network, to determine a suitable cutoff for

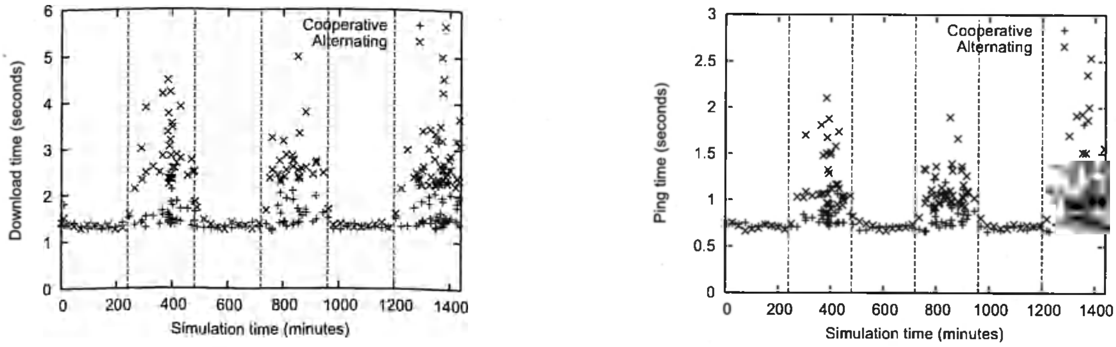


Fig. 9. Average download and ping time with relays that alternate between being cooperative and selfish. This experiment is with gold star scheme in place and heavy background traffic (20 BitTorrent clients and 2000 web clients). Dotted lines show the times at which the alternating relays switch. The performance of alternating relays gets worse whenever they switched to being selfish, while that for cooperative relays only suffers a little.

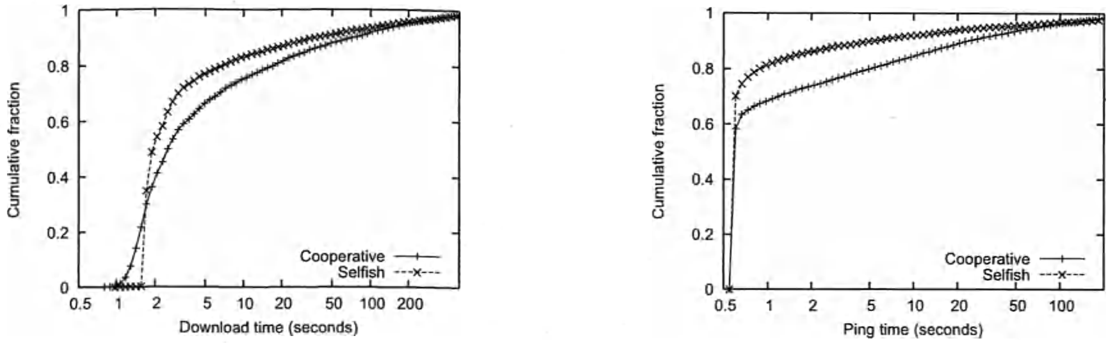


Fig. 10. Cumulative download and ping time with the pair-wise reputation design and heavy traffic (20 BitTorrent clients and 2000 web clients). Four relay types (cooperative, selfish, cooperative reserve, and adaptive) are simulated, although only the performance of the former two are shown, as the latter two behave similarly to cooperative relays.

granting gold stars (see Section VI-A for more discussion on handling strategic behaviors in Tor).

D. Experiment 3: Alternating Relays

This experiment considers a variation on the adaptive strategy, used previously. Alternating nodes will toggle between the cooperative and the selfish strategies on a longer timescale—four hours per switch. This experiment uses 50 such alternating relays with 50 cooperative relays and with heavy background traffic (20 BitTorrent clients and 2000 web clients).

Figure 9 shows the average download and ping time for both relay types over time. During the periods where the alternating relays are cooperative, they receive service of a similar quality as the full-time cooperative nodes. However, once the alternating relays switch to become selfish, their download times quickly increase, representing the same quality of service that would be observed by a selfish node. Of interest, while the cooperative nodes do observe lower quality of service (after all, fully half of the Tor nodes stopped relaying any data), they still do much better than their selfish peers.

This experiment further demonstrates our gold star system robustly responding to changes in node behavior.

E. Experiment 4: Pair-wise Reputation

In this final experiment, we investigated a variation on our gold star design, where individual circuits are not labeled as being low or high priority. In this variation, a low-priority node routing traffic through a gold-star node will experience priority delays getting the gold-star node to accept the traffic, but the traffic will have the gold-star priority in its subsequent hops. This alternative design has significant improvements from an anonymity perspective, because traffic at a given hop doesn't give any hint about whether it originated from a low-priority or high-priority node. However, this design might fail from an incentives perspective, since there is less incentive for a node to earn its own gold star.

In this experiment, we again simulate a network with 40 relays for each relay type: cooperative, selfish, cooperative reserve, and adaptive. For clarity, Figure 10 only shows the download and ping time for cooperative and selfish relays, as the performance for cooperative reserve and adaptive relays is very close to that for cooperative relays.

This experiment shows selfish nodes clearly outperforming their cooperative peers. This indicates that the gold star strategy requires a transitive property, i.e., each hop of a circuit must inherit the gold star status of the previous hop. Otherwise, selfish nodes will outperform their cooperative peers and there will be no incentive for cooperation.

VI. Discussion

Our experiments show that our "gold star" technique is effective at giving higher priority to users who contribute to the Tor network. Nonetheless, a variety of interesting concerns remain about the exact policy that should be used for giving and taking away gold stars and how these may affect the behavior of strategic Tor users.

A. Strategic users

Our proposed incentive scheme is not perfectly strategy-proof, in the sense that users can earn a gold star without providing *all* of their network capacity for the use of the Tor network. With present-day Tor, relays are either altruistic or adversarial, i.e., some Tor relays will behave correctly, while others will behave in an arbitrary fashion, perhaps to perform anonymity attacks by observing traffic at the edges of the network, or to perform other attacks by observing or modifying sensitive data as it exits the Tor network. Our incentives design introduces a third class of relay: users who try to earn a gold star without being entirely cooperative. Here we describe some variants on this strategic user.

1) Provide borderline or spotty service: A relay need provide only the minimal amount of bandwidth necessary to gain the gold star. First, note that if every user provided this amount, Tor would still have vastly greater resources than it does today. Next, because the bandwidth policies are determined centrally, the minimum bandwidth necessary to obtain a gold star could be moved up or down manually. Likewise, central authorities could perform latency tests or make other dynamic measurements to sample the load factor on the Tor network and could then adjust the gold star threshold dynamically, without administrative involvement. Assuming these limits are made public, strategic nodes could then adjust the resources they provide to the network to maintain their gold stars, making more bandwidth available whenever they are needed. Thus we convert these borderline relays into cooperative servers.

2) Only relay at strategic times: Such users might provide relay services only prior to the user's own desire to use the Tor network. This speaks to a need to stretch the length of time or the number of successful audits that must be passed before a Tor relay is granted a gold star. Even then, a user who follows a regular daily schedule could plan around this, arranging for their Tor relay to join the system well before they got home from the day at work. Such behavior is not disincentivized by our research, as it still provides scalable resources to the Tor network. However, any users following such behavior may be partially compromising their anonymity, as any deviations from their normal behavior will be externally observable.

3) Share a relay among several users: Several users could share a single entry relay into the Tor network, thus inheriting its gold star benefits without providing any additional bandwidth to the Tor network. In fact, we may even want to support this design, so users can run a fast relay at a colocation facility and then reap the rewards from their slower cable-modem or DSL Tor client. To allow the client to inherit the reputation of the server, the relay could be configured to give high priority to allow connections from a given set of IP addresses or identity keys. On the other hand, multiple users that use a shared entry point must be able to trust one another. Lacking such trust, their desire for personal anonymity would incentivize them to run individual Tor relays.

4) Accept traffic only from known relays: In our design the directory authorities do their measurements anonymously via Tor, so all audits will come from other listed Tor relays. Thus a strategic relay could get away with giving poor performance (or no performance at all!) to connections from IP addresses not listed in the directory. One answer is that some of the measurements should be done through sources other than the known relays, perhaps by gathering a large pool of volunteer Tor users to help diversify the audit sources. Another answer is to turn this vulnerability around and call it a feature—another reason that users should want to get listed as a relay.

5) Forward high-priority traffic as low-priority: A relay who correctly forwards traffic can still cheat by changing the priority on incoming traffic. By doing so he makes more room for his own outgoing high-priority traffic. The measuring authorities could then perform low and high-priority audits, comparing the results. They might also try building high-priority circuits through the relay being tested and then back to a trusted relay (with a hop in between for better anonymity), to see if the circuit arrives with the expected high-priority status.

6) Sequential colluding relays: A circuit that happens to traverse two colluding relays will give these relays a better chance of predicting whether the circuit is performing an audit. The relays could then give preferential service during a suspected audit, and degraded service otherwise. We rely on repeated audits, along the low probability that we repeatedly pick colluding nodes in a circuit, to limit the probability that this type of cheating will make a significant difference.

B. The audit arms race

Many of the attacks outlined above involve relays that provide some level of service but not quite as much as expected. The response in each case is a smarter or more intensive measurement algorithm so the directory authorities can more precisely distinguish between a cooperating relay and a not-entirely-cooperating relay.

To see why this won't be an infinitely spiraling arms race between increasingly subtle cheating and increasingly sophisticated audits, we need to examine the incentives for ordinary users. The most challenging part of setting up a Tor relay is configuring the software, enabling port forwarding in the firewall, etc. Compared to this initial barrier, the incremental cost of providing a bit more bandwidth is low for most users. Therefore as long as our audit mechanism correctly judges whether the user relays any traffic at all, we're verifying that the user has performed the most costly step in setting up relaying. We expect that the diminishing returns a strategic relay gets in saving bandwidth as we progress down the arms race will limit the complexity required for the auditing mechanism.

Measuring whether a relay is forwarding traffic adequately within the network is only one step. We could also extend our auditing techniques to measure whether an exit relay is in fact correcting forwarding exit traffic. A strategic exit relay, interested in reducing its bandwidth expenses or in avoiding abuse complaints, might cut off some or all connections, perhaps returning "not found" messages rather than performing an actual web lookup. Once our audits can distinguish correctly performing exit relays, we could either assign gold stars more leniently to the relays that also allow exit traffic, or we could add a third class of service for "extra high" priority traffic.

But how do we come up with convincing exit traffic tests that aren't trivially distinguishable from real exit traffic? We leave the details to future work, but we speculate that it would involve both requests to common sites (such as a Google search on a random word) and user-submitted tests. The results would be compared to the same tests performed over a different circuit, or even tests performed directly without Tor.

Finally, our proposed audits could be augmented by "charging" the entry and exit nodes in a bandwidth measurement probe if the result is faulty. As circuits are rebuilt differently on each probe, eventually the truly faulty nodes will stand out by having a higher fault rate. Such "collateral reputation damage" designs must be considered with care, as an adversarial relay can damage the reputation of specific target relays by preferentially failing circuits that involve those relays; this ability to influence reputation can assist in anonymity-breaking attacks [4], [18].

C. Anonymity implications

While it is difficult to quantify anonymity in low-latency designs or to state definitively that one design is better or worse at preserving anonymity than another, we can certainly discuss the relative effects on Tor's anonymity once our two-class structure is imposed on the network. It's reasonable to assume that some large number of clients will be unimpressed with the performance improvements from holding a gold star or will otherwise be unable or unwilling to run a Tor relay of their own.

As such, the Tor network could well only have a small number of gold star relays. Whenever a Tor relay receives a high priority cell, it knows with absolute certainty that the cell must have originated from a relay having a gold star. With so few gold star relays, the presence of high priority traffic greatly reduces the number of possible sources for that traffic. Worse, the set of users with a gold star is made public, whereas (Section II-C notwithstanding) it is relatively hard to build a list of every Tor user out there.

We believe this tradeoff is acceptable for several reasons. First, altruists would be the early adopters, as predicted by Acquisti et al. [1] and as observed in the current Tor network. Low-sensitivity users would come next; many users who care more about performance than anonymity would be enticed into running Tor relays and getting gold stars. The number of gold star nodes in the system should therefore increase over time, reducing the extent to which the presence of prioritized traffic gives away useful information to an eavesdropper. Likewise, as getting a gold star inherently requires participating in the Tor network, our system should significantly increase the number of relays in the Tor network, thus improving the anonymity of all Tor users. We speculate that the growing anonymity set of gold star relays, along with the improved performance from being in the group getting priority traffic, would ultimately be enough to push even the high-sensitivity users into setting up relays.

Note that as we attract more relays, the anonymity that can be achieved increases for both the relays and the clients; we explore this economics perspective in Section VI-D below.

Is it possible to blur the anonymity sets, so receiving a circuit with a given priority still leaves the attacker some uncertainty about the anonymity set of its origin? We first considered the possibility of assigning and/or removing gold stars at random, adding further uncertainty to an attackers' ability to gain meaningful information about the source of high-priority traffic. This perturbation could be implemented both by the directory authority or within individual Tor relays. We ultimately rejected this approach because it incentivizes users to create large numbers of circuits in the hopes that one of them may, through good luck, be high priority. Such behavior would be wasteful of network resources and would defeat incentives mechanisms.

Is it possible to hide the set of relays that have earned a gold star, so an attacker doesn't have a complete list of suspects? Cryptography could allow the directory authorities to provide a signed blinded token to relays that deserve a gold star, and then entry nodes would check the token in a decentralized fashion without need for the central directory. Of course, gold star relays have to be in the public list of Tor relays anyway, so they can be discovered and used in the first place. As such, the incremental damage to a users' anonymity from being a gold star relay relative to the damage from being a relay at all is fairly minimal.

D. The economics of attracting more relays

Our simulations in the previous sections examine various static combinations of agents, and show that with some combinations, the relays with gold stars get significantly improved performance relative to the other agents.

That's not the whole story, though. By encouraging users to enable relaying, we aren't just trying to separate cooperative users from freeloaders; rather, we're trying to convert freeloaders into cooperative users, and thereby grow the capacity of the network. That is, we aim to shift the network from one where there isn't enough capacity to one where there is excess capacity. Such a network can in turn provide increased performance even for users that don't or can't enable relaying; everybody wins, both from a performance and from an anonymity perspective.

However, this brief discussion of the economic aspect of our incentive strategy leaves out a lot of details. We might want to start by analyzing the various equilibria and deriving utility functions for various user classes. We leave this investigation to future work.

E. Extensions

Our experiments show that our design creates significant incentives for users to run Tor relays. In practice, it might occur that the observable performance difference between high priority traffic and regular traffic is insufficient, perhaps due to excess network capacity. If such a problem were to occur, one additional possibility would be to reserve bandwidth for high-priority traffic [37], effectively throttling low-priority traffic and creating a larger incentive for users to get a gold star. The downside to such an approach, of course, is that Tor performance would "needlessly" suffer for low-priority Tor users.

Another possible extension would be to implement higher priorities for interactive traffic versus bulk data transfers. Web surfing is highly sensitive to latency, while bulk transfer protocols like BitTorrent are relatively insensitive to it. Such behavior is comparable to "traffic shaping" devices now being widely deployed. If BitTorrent and other file transfer traffic through Tor is sufficiently slow and unusable, then the BitTorrent developers will (hopefully) have the incentive to design their own anonymity mechanism. On the other hand, it's unclear how to achieve these different priorities: BitTorrent is resistant to schemes that throttle high-volume streams, since it automatically shifts load to new streams, and running protocol identification tools on the exit relays is a slippery slope with respect to wiretapping and liability.

VII. Related Work

A. Incentives in anonymous communication networks

Anonymous communication networks in practice have operated primarily based on three incentive approaches: *community support*, *payment for service*, and *government support*. (Discussion of the funding approaches for research and development of anonymity designs, while related, is outside the scope of this paper.)

The Tor network right now is built on community support: a group of volunteers from around the Internet donate their resources because they want the network to exist.

Zero-Knowledge Systems' Freedom network [5] on the other hand was a commercial anonymity service. They collected money from their users, and paid commercial ISPs to relay traffic. While that particular company failed to make its business model work, the more modest Anonymizer [2] successfully operates a commercial one-hop proxy based on a similar approach.

Lastly, the AN.ON project's cascade-based network is directly funded by the German government as part of a research project. Unfortunately, the funding ends in 2007, so they are exploring the community support approach (several of their nodes are now operated by other universities) and the pay-for-play approach (setting up commercial cascades that provide more reliable service).

Other incentive approaches have been discussed as well. Acquisti et al. [1] argued that high-needs users (people who place a high value on their anonymity) will opt to relay traffic in order to attract low-needs users — and that some level of free riding is actually beneficial because it provides cover traffic to blend with. It's unclear how well that argument transitions from the high-latency systems analyzed in that paper to low-latency systems, especially since the different threat models change the incentive structure.

B. Incentives in other peer-to-peer networks

1) Incentives for applications: Incentive schemes have been proposed for several other peer-to-peer applications. BitTorrent [7] is one of the pioneers. It facilitates large numbers of nodes trying to share the effort of downloading very large files. Every BitTorrent node will have acquired some subset of the file and will trade blocks with other nodes until it has the rest. Nodes will preferentially trade blocks with peers that give them better service ("tit-for-tat" trading). Scrivener [34] addresses a more general problem, where nodes are interested in content from a large set of potentially much smaller size.

In a storage network, nodes share spare disk capacity for applications such as distributed backup systems. Ngan et al. [35] propose an auditing mechanism, which allows cheaters to be discovered and evicted from the system. Samsara [8] enforces fairness by requiring an equal exchange of storage space between peers and by challenging peers periodically to prove that they are actually storing the data. Tangler [44] requires users to provide resources for a probation period before they are allowed to consume resources, similar in spirit to our gold star design.

2) Reputation systems: Resource allocation and accountability problems are fundamental to peer-to-peer systems. Dingledine et al. [13] surveys many schemes for tracking nodes' reputations. In particular, if obtaining a new identity is cheap and positive reputations have value, negative reputation could be shed easily by leaving the system and rejoining with a new identity. Friedman and Resnick [21] also study the case of cheap pseudonyms, and argue that suspicion of strangers is costly. EigenTrust [27] is a distributed algorithm for nodes to securely compute global trust values based on their past performance. Blanc et al. [3] suggest a reputation system for incentivizing routing in peer-to-peer networks that uses a trusted authority to manage the reputation values for all peers, comparable to our use of directory authorities.

3) Trading and payments: SHARP [22] is a framework for distributed resource management, where users can trade resources like bandwidth with trusted peers. KARMA [43] and SeAl [36] rely on auditor sets to keep track of the resource usage of each participant in the network. Golle et al. [23] considered centralized peer-to-peer systems with micro-payments, analyzing how various user strategies reach equilibrium within a game theoretic model.

VIII. Integrating our design into Tor

We now discuss pragmatic issues that we will face as we adapt our techniques to run on the actual Tor network.

A. Implementing priorities

The Tor implementation presently has support for rate limiting but has no notion of traffic priorities. We would need to extend Tor to support priorities both for the local user and for remote gold star traffic.

Presently, Tor sets up a single TCP connection between pairs of nodes, with cells from multiple circuits routed across these shared TCP connections. Tor then relies on TCP for rate limiting on individual connections. How can Tor distinguish whether the next cell on a socket is low or high priority?

We could set up two separate TCP connections, but this lets an observer possibly distinguish local traffic (always high priority) from relayed traffic (either high or low). Given that we must use a single TCP connection, we can adopt a variety of different policies. For example, we might adopt a policy of reading at most one low priority cell at a time before moving on to the next socket, versus reading many cells at a time, so long as they are all for high priority circuits. One attractive solution is to adopt a separate control channel and data channel (both encrypted). The control channel could specify the priorities of upcoming cells, allowing the receiver to compute priorities in advance. On the sending side, selecting the cell ordering on a TCP socket is a standard priority queuing problem, with many possible approaches to evaluate.

We likewise wish to support policies similar to our "cooperative reserve" model, where some bandwidth is reserved for "local" traffic. This will similarly require varying the cell priorities and tracking which inbound sockets have lately had local data on them. We would then read more cells at a time from sockets with higher "locality." If the control channel specified each cell's circuit ID as well as its priority, this would be straightforward to implement.

B. Directory authority changes

The changes required in the directory protocol are quite straightforward. We would add a new "priority" flag to each router's entry in Tor's network status documents, and each authority would provide a vote in its network status about whether each relay should receive the flag.

While Tor's directory authorities simply do reachability testing right now, we would want to ramp that up so they can do more sophisticated measurements. TorFlow [39], a tool that automatically builds paths through the Tor network and measures the bandwidth received, can already do most of the work. TorFlow even has experimental features that test exit traffic to check whether SSL certs from destination websites are as expected.

Our simulations look over a short period of time (one day) and assume directory authorities make frequent measurements (ten authorities, each performing one measurement probe every minute). While this setting responds quickly to changing behavior, it may not remain feasible as the network scales. Furthermore, Tor would benefit more from long-term stable nodes than from short-term bursts of available bandwidth. Thus we should prepare for a lower sampling rate in the real Tor network. A node wanting a gold star would need to provide consistent service for days, rather than for hours. A longer-term sampling period would also allow nodes to preserve their gold stars, even if they experience transient failures that disconnect them from the network.

IX. Conclusions

This paper proposes an incentive scheme to reward Tor users who relay traffic. Simulations show that such relays can get significant performance improvements. Our design initially reduces anonymity for these relays, but we argue that this is an acceptable tradeoff, and we speculate that ultimately both relays and clients will see improved performance and improved anonymity.

We have identified some areas for further research, such as how to reward relays without separating anonymity sets as much, how to scale up the audits to work on a large Tor network, what thresholds should merit a gold star, whether we need to do simulations that reflect a more realistic mix of users (e.g. more slow relays and/or relays with asymmetric bandwidth), and how exactly to implement priority for circuits as described in Section VIII. Once these issues have been investigated, we should integrate our design into an upcoming Tor release and test how well it works in real network conditions.

References

[1] Alessandro Acquisti, Roger Dingledine, and Paul Syverson. On the economics of anonymity. In *Proceedings of the 7th Annual Conference on Financial Cryptography (FC '03)*, Gosier, Guadeloupe, January 2003.

[2] The Anonymizer. http://www.anonymizer.com/.

[3] Alberto Blanc, Yi-Kai Liu, and Amin Vahdat. Designing incentives for peer-to-peer routing. In *Proceedings of the 24th IEEE INFOCOM*, Miami, FL, March 2005.

[4] Nikita Borisov, George Danezis, Prateek Mittal, and Parisa Tabriz. Denial of service or denial of security? How attacks on reliability can compromise anonymity. In *Proceedings of CCS 2007*, October 2007.

[5] Philippe Boucher, Adam Shostack, and Ian Goldberg. Freedom systems 2.0 architecture. White paper, Zero Knowledge Systems, Inc., December 2000. http://osiris.978.org/~brianr/crypto-research/anon/www.freedom.net/products/whitepapers/Freedom_System_2_Architecture.pdf.

[6] David Chaum. The dining cryptographers problem: Unconditional sender and recipient untraceability. *Journal of Cryptology*, 1(1):65–75, 1988.

[7] Bram Cohen. Incentives build robustness in BitTorrent. In *Proceedings of the Workshop on Economics of Peer-to-Peer Systems*, Berkeley, CA, June 2003.

[8] Landon P. Cox and Brian D. Noble. Samsara: Honor among thieves in peer-to-peer storage. In *Proceedings of the 19th ACM Symposium on Operating System Principles (SOSP '03)*, Bolton Landing, NY, October 2003.

[9] Mark E. Crovella and Azer Bestavros. Self-similarity in world wide web traffic: Evidence and possible causes. *IEEE/ACM Transactions on Networking*, 5(6):835–846, 1997.

[10] Wei Dai. PipeNet 1.1. Post to Cypherpunks mailing list, November 1998. http://www.eskimo.com/~weidai/pipenet.txt.

[11] George Danezis. The traffic analysis of continuous-time mixes. In *Proceedings of Privacy Enhancing Technologies workshop (PET 2004)*, volume 3424 of *LNCS*, pages 35–50, Toronto, Canada, May 2004.

[12] George Danezis, Roger Dingledine, and Nick Mathewson. Mixminion: Design of a type III anonymous remailer protocol. In *Proceedings of the IEEE Symposium on Security and Privacy*, Oakland, CA, May 2003.

[13] Roger Dingledine, Michael J. Freedman, and David Molnar. Accountability measures for peer-to-peer systems. In *Peer-to-Peer: Harnessing the Power of Disruptive Technologies*. O'Reilly and Associates, November 2000.

[14] Roger Dingledine and Nick Mathewson. Tor protocol specification. https://www.torproject.org/svn/trunk/doc/spec/tor-spec.txt.

[15] Roger Dingledine and Nick Mathewson. Anonymity loves company: Usability and the network effect. In *Proceedings of the Fifth Workshop on the Economics of Information Security (WEIS 2006)*, Cambridge, UK, June 2006.

[16] Roger Dingledine, Nick Mathewson, and Paul Syverson. Tor: The second-generation onion router. In *Proceedings of 13th USENIX Security Symposium*, San Diego, CA, August 2004. Project web site: https://www.torproject.org/.

[17] Roger Dingledine, Nick Mathewson, and Paul Syverson. Challenges in deploying low-latency anonymity. Technical Report 5540-265, Center for High Assurance Computer Systems, Naval Research Laboratory, 2005.

[18] Roger Dingledine and Paul Syverson. Reliable MIX cascade networks through reputation. In *Proceedings of the 6th Annual Conference on Financial Cryptography (FC '02)*, Southampton, Bermuda, March 2002.

[19] John R. Douceur. The Sybil Attack. In *Proceedings of 1st International Workshop on Peer-to-Peer Systems (IPTPS)*, Cambridge, MA, March 2002.

[20] Electronic Frontier Foundation. Tor: Legal FAQ for Tor server operators. https://www.torproject.org/eff/tor-legal-faq.html.

[21] Eric Friedman and Paul Resnick. The social cost of cheap pseudonyms. *Journal of Economics and Management Strategy*, 10(2):173–199, 2001.

[22] Yun Fu, Jeffrey S. Chase, Brent N. Chun, Stephen Schwab, and Amin Vahdat. SHARP: An architecture for secure resource peering. In *Proceedings of the 19th ACM Symposium on Operating System Principles (SOSP '03)*, Bolton Landing, NY, October 2003.

[23] Philippe Golle, Kevin Leyton-Brown, Ilya Mironov, and Mark Lillibridge. Incentives for sharing in peer-to-peer networks. In *Proceedings of the 3rd ACM Conference on Electronic Commerce*, Tampa, FL, October 2001.

[24] Garrett Hardin. The tragedy of the commons. *Science*, 162, 1968. Alternate location: http://dieoff.com/page95.htm.

[25] Felix Hernández-Campos, Kevin Jeffay, and F. Donelson Smith. Tracking the evolution of web traffic: 1995–2003. In *Proceedings of the 11th IEEE/ACM International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS)*, Orlando, FL, October 2003.

[26] Nicholas Hopper, Eugene Y. Vasserman, and Eric Chan-Tin. How much anonymity does network latency leak? In *Proceedings of the 14th ACM Conference on Computer and Communication Security*, Alexandria, VA, October 2007.

[27] Sepandar D. Kamvar, Mario T. Schlosser, and Hector Garcia-Molina. The EigenTrust algorithm for reputation management in p2p networks. In *Proceedings of the 12th International World Wide Web Conference*, Budapest, Hungary, May 2003.

[28] Brian N. Levine, Michael K. Reiter, Chenxi Wang, and Matthew K. Wright. Timing attacks in low-latency mix-based systems. In *Proceedings of the 8th Annual Conference on Financial Cryptography (FC '04)*, Key West, Florida, February 2004.

[29] Marc Liberatore and Brian Neil Levine. Inferring the Source of Encrypted HTTP Connections. In *Proceedings of the 13th ACM conference on Computer and Communications Security (CCS 2006)*, pages 255–263, Alexandria, VA, October 2006.

[30] Sergio Marti, Prasanna Ganesan, and Hector Garcia-Molina. SPROUT: P2P routing with social networks. In *First International Workshop on Peer-to-Peer and Databases (P2PDB 2004)*, Springer LNCS 3268, pages 425–435, Heraklion, Greece, March 2004.

[31] Ulf Möller, Lance Cottrell, Peter Palfrader, and Len Sassaman. Mixmaster protocol — version 2. IETF Internet Draft, July 2003. http://www.abditum.com/mixmaster-spec.txt.

[32] Steven J. Murdoch and George Danezis. Low-cost traffic analysis of Tor. In *Proceedings of the IEEE Symposium on Security and Privacy*, Oakland, CA, May 2005.

[33] Steven J. Murdoch and Piotr Zieliński. Sampled traffic analysis by internet-exchange-level adversaries. In *Proceedings of Privacy Enhancing Technologies Symposium (PET 2007)*, Ottawa, Canada, June 2007.

[34] Animesh Nandi, Tsuen-Wan "Johnny" Ngan, Atul Singh, Peter Druschel, and Dan S. Wallach. Scrivener: Providing incentives in cooperative content distribution systems. In *Proceedings of the ACM/IFIP/USENIX 6th International Middleware Conference (Middleware 2005)*, Grenoble, France, November 2005.

[35] Tsuen-Wan "Johnny" Ngan, Dan S. Wallach, and Peter Druschel. Enforcing fair sharing of peer-to-peer resources. In *Proceedings of the 2nd International Workshop on Peer-to-Peer Systems (IPTPS)*, Berkeley, CA, February 2003.

[36] Nikos Ntarmos and Peter Triantafillou. SeAl: Managing accesses and data in peer-to-peer sharing networks. In *Proceedings of the 4th IEEE International Conference on P2P Computing*, Zurich, Switzerland, August 2004.

[37] Andrew M. Odlyzko. Paris metro pricing for the Internet. In *ACM Conference on Electronic Commerce*, pages 140–147, 1999.

[38] Lasse Øverlier and Paul Syverson. Locating hidden servers. In *Proceedings of the IEEE Symposium on Security and Privacy*, Oakland, CA, May 2006.

[39] Mike Perry and Johannes Renner. TorFlow. https://www.torproject.org/svn/torflow/README.

[40] Vitaly Shmatikov and Ming-Hsui Wang. Timing analysis in low-latency mix networks: Attacks and defenses. In *Proceedings of the 11th European Symposium On Research In Computer Security (ESORICS 2006)*, Hamburg, Germany, September 2006.

[41] Atul Singh, Tsuen-Wan "Johnny" Ngan, Peter Druschel, and Dan S. Wallach. Eclipse attacks on overlay networks: Threats and defenses. In *Processings of IEEE INFOCOM*, Barcelona, Spain, April 2006.

[42] The Distributed and Real-Time Systems Research Group, UNC. Data for the UNC HTTP traffic model. http://www.cs.unc.edu/Research/dirt/proj/http-model/.

[43] Vivek Vishnumurthy, Sangeeth Chandrakumar, and Emin Gün Sirer. KARMA: A secure economic framework for p2p resource sharing. In *Proceedings of the Workshop on Economics of Peer-to-Peer Systems*, Berkeley, CA, June 2003.

[44] Marc Waldman and David Mazières. Tangler: A censorship resistant publishing system based on document entanglements. In *Proceedings of the 8th ACM Conference on Computer and Communication Security (CCS 2001)*, Philadelphia, Pennsylvania, November 2001.

[45] Haifeng Yu, Michael Kaminsky, Phillip B. Gibbons, and Abraham Flaxman. SybilGuard: Defending against Sybil attacks via social networks. In *Proceedings of ACM SIGCOMM '06*, Pisa, Italy, September 2006.

```
|Time     | client                           |
|         |                  | tor-server       |
|26.447   |        50941 > https [SYN]         |TCP: 50941 > https [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=3
TSV=308243361 TSER=0
|         |(50941) ------------------> (443)   |
|26.808   |        https > 50941 [SYN,         |TCP: https > 50941 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0
MSS=1412 TSV=48279126 TSER=308243361 WS=6
|         |(50941) <------------------ (443)   |
|26.809   |        50941 > https [ACK]         |TCP: 50941 > https [ACK] Seq=1 Ack=1 Win=524280 Len=0
TSV=308243364 TSER=48279126
|         |(50941) ------------------> (443)   |
|26.809   |        Client Hello               |SSL: Client Hello
|         |(50941) ------------------> (443)   |
|27.272   |        https > 50941 [ACK]         |TCP: https > 50941 [ACK] Seq=1 Ack=145 Win=6912 Len=0
TSV=48279217 TSER=308243364
|         |(50941) <------------------ (443)   |
|56.118   |        50941 > https [FIN,         |TCP: 50941 > https [FIN, ACK] Seq=145 Ack=1 Win=524280 Len=0
TSV=308243657 TSER=48279217
|         |(50941) ------------------> (443)   |
|57.054   |        50941 > https [FIN,         |TCP: 50941 > https [FIN, ACK] Seq=145 Ack=1 Win=524280 Len=0
TSV=308243666 TSER=48279217
|         |(50941) ------------------> (443)   |
|59.055   |        50941 > https [FIN,         |TCP: 50941 > https [FIN, ACK] Seq=145 Ack=1 Win=524280 Len=0
TSV=308243686 TSER=48279217
|         |(50941) ------------------> (443)   |
|63.058   |        50941 > https [FIN,         |TCP: 50941 > https [FIN, ACK] Seq=145 Ack=1 Win=524280 Len=0
TSV=308243726 TSER=48279217
|         |(50941) ------------------> (443)   |
|71.061   |        50941 > https [FIN,         |TCP: 50941 > https [FIN, ACK] Seq=145 Ack=1 Win=524280 Len=0
TSV=308243806 TSER=48279217
|         |(50941) ------------------> (443)   |
|87.066   |        50941 > https [FIN,         |TCP: 50941 > https [FIN, ACK] Seq=145 Ack=1 Win=524280 Len=0
TSV=308243966 TSER=48279217
|         |(50941) ------------------> (443)   |
|119.077  |        50941 > https [FIN,         |TCP: 50941 > https [FIN, ACK] Seq=145 Ack=1 Win=524280 Len=0
TSV=308244286 TSER=48279217
|         |(50941) ------------------> (443)   |
|183.096  |        50941 > https [FIN,         |TCP: 50941 > https [FIN, ACK] Seq=145 Ack=1 Win=524280 Len=0
TSV=308244926 TSER=48279217
|         |(50941) ------------------> (443)   |
|247.118  |        50941 > https [FIN,         |TCP: 50941 > https [FIN, ACK] Seq=145 Ack=1 Win=524280 Len=0
TSV=308245566 TSER=48279217
|         |(50941) ------------------> (443)   |
|311.145  |        50941 > https [FIN,         |TCP: 50941 > https [FIN, ACK] Seq=145 Ack=1 Win=524280 Len=0
TSV=308246206 TSER=48279217
|         |(50941) ------------------> (443)   |
|375.168  |        50941 > https [FIN,         |TCP: 50941 > https [FIN, ACK] Seq=145 Ack=1 Win=524280 Len=0
TSV=308246846 TSER=48279217
|         |(50941) ------------------> (443)   |
|439.192  |        50941 > https [FIN,         |TCP: 50941 > https [FIN, ACK] Seq=145 Ack=1 Win=524280 Len=0
TSV=308247486 TSER=48279217
|         |(50941) ------------------> (443)   |
|503.219  |        50941 > https [FIN,         |TCP: 50941 > https [FIN, ACK] Seq=145 Ack=1 Win=524280 Len=0
```

```
TSV=308248126 TSER=48279217
|         |(50941)  ------------------>  (443)    |
|567.292  |         50941 > https [RST,           |TCP: 50941 > https [RST, ACK] Seq=146 Ack=1 Win=524280 Len=0
|         |(50941)  ------------------>  (443)    |
```