General Overview:
U.S. Government Executive Branch Information Assurance (IA)
Acquisition Policies and Source Code Requirements
February 21, 2006

Generally speaking, U.S. Government (USG) executive branch agencies (see Attachment A for list of these agencies) require source code review in government information security and information assurance (IA) procurement only in certain select cases. Please see below.

Non-national security versus national security computer systems: USG executive branch agency computer systems are categorized by a legal definition (see Attachment B) as either national security or non-national security systems. This categorization is not by agency, but by computer system. Even a "national security"-related agency, such as the U.S. Department of Defense (DOD) or the Department of Homeland Security (DHS), will have both national security and non-national security computer systems. The level of security for each type of system is distinct.

NON-NATIONAL SECURITY COMPUTER SYSTEMS:
The vast majority of USG computer systems fall into this category.

NIST standards and guidelines: The Federal Information Security Management Act (FISMA) of 2002 mandates that executive branch agencies that handle sensitive but non-classified materials must use computer security standards and guidelines developed by the National Institute of Standards and Technology (NIST). NIST's Computer Security Division creates and disseminates these standards and guidelines, using extensive private-sector input, such as via public comment procedures. NIST's standards for federal computer systems are called Federal Information Processing Standards Publications (FIPS PUBS), and the guidelines are the Special Publication 800 (SP-800) series.

NIST's standards and guidelines for federal government computer security are found here: http://csrc.nist.gov/publications/index.html

Source code is almost never required to meet these NIST standards and guidelines, with one specific exception for cryptographic modules, FIPS-140-2.

NIST's FIPS 140-2, "Security Requirements for Cryptographic Modules," is applicable to all Federal agencies that use cryptographic-based security systems to protect sensitive information in computer and telecommunication systems (including voice systems) as defined in Section 5131 of the Information Technology Management Reform Act of 1996, Public Law 104-106. Cryptographic commercial-off-the-shelf (COTS) products used by the USG must be validated to FIPS 140-2 by the NIST Cryptographic Module Validation Program (CMVP). All of the tests under the CMVP are handled by third-party laboratories that are accredited as Cryptographic Module Testing (CMT) laboratories by the National Voluntary Laboratory Accreditation Program (NVLAP). All FIPS 140-2 testing that is performed by a testing laboratory includes review of any and

all source code that is part of the cryptographic module. However, the code is provided only to the laboratory (not to NIST) under a non-disclosure agreement. NIST would only have access to see source code if the CMVP specifically requested such code during the validation review of the test results provided by the laboratory (during a validation review, the CMVP may request more details). NIST's access to source code in such an instance would also be bound by the same non-disclosure through the NVLAP. Further, the modules are generally small enough to make code examination feasible. CMVP assumes that once a module has been validated, that very same module (unchanged/not tampered with) is in every product the vendor sells, and therefore there is no need to test specific purchases (i.e., the vendor is trusted to put the approved/tested module in every product without modification).

Information on the CMVP is found here: http://csrc.nist.gov/cryptval/

Federal Acquisition Regulation (FAR): The FAR, which complements FISMA, governs USG non-national security procurement contracts. With a few exceptions, the majority of USG executive branch agencies are bound by, and must purchase in accordance with, the FAR.

FAR section 12.212 applies to purchases of COTS computer software, and mandates that USG agencies, when purchasing such software, must accept the commercial license or end-user-licensing agreement. This section is copied below:

> *12.212 Computer software.*
> *(a) Commercial computer software or commercial computer software documentation shall be acquired under licenses customarily provided to the public to the extent such licenses are consistent with Federal law and otherwise satisfy the Government's needs. Generally, offerors and contractors shall not be required to—*
> *(1) Furnish technical information related to commercial computer software or commercial computer software documentation that is not customarily provided to the public; or*
> *(2) Relinquish to, or otherwise provide, the Government rights to use, modify, reproduce, release, perform, display, or disclose commercial computer software or commercial computer software documentation except as mutually agreed to by the parties.*
>
> *(b) With regard to commercial computer software and commercial computer software documentation, the Government shall have only those rights specified in the license contained in any addendum to the contract.*

In item (1) above, source code is considered to be an example of "technical information" that offerors and contractors are not required to furnish.

General information on the FAR is found at: http://205.130.237.11/far/

NATIONAL SECURITY COMPUTER SYSTEMS:
NIST's standards and guidelines and the FAR do not apply to national security agencies or national security computer systems. For information assurance procurement by national security agencies or national security computer systems, agencies must follow "NSTISSP #11." NSTISSP 11 is a national security community policy governing the acquisition of information assurance (IA) and IA-enabled information technology products. The policy mandates, effective 1 July 2002, that departments and agencies within the Executive Branch shall acquire, for use on national security systems, only those COTS products or cryptographic modules that have been validated with the International Common Criteria for Information Technology Security Evaluation, the National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS), or by the National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) Cryptographic Module Validation Program.

The objective of NSTISSP #11 is to ensure that COTS IA and IA-enabled IT products acquired by the U.S. Government for use in national security systems perform as advertised by their respective manufacturers, or satisfy the security requirements of the intended user.

Information on NSTISSP 11 is found at: http://niap.nist.gov/cc-scheme/nstissp-faqs.html

Source code review: Even when following NSTISSP 11, only in certain procurement cases is source code review or submission required. These instances would be:

- Department of Defense: Department of Defense Directive (DoDD) 8500.1 and Department of Defense Instruction (DoDI) 8500.2 define the protection requirements and the implementation of NSTISSP#11. These documents call for the acquisition of products that have been evaluated against a CC Protection Profile based on 3 levels of robustness (basic, medium, and high). Protection Profiles at the medium and high robustness levels include vulnerability analysis requirements, and require the vendor to provide source code for review (i.e., AVA-VLA.3 at EAL5 requires source code).
- If the cryptographic module is tested under FIPS 140-2 and validated by the CMVP, as explained above.

The only other occasion where the USG may ask for source code is when the USG pays for the code to be written so that it becomes the government's intellectual property (IP), as opposed to IP of the vendor.

Attachment A: U.S. Executive Branch

Executive Office of the President (EOP)
White House
Office of Management and Budget (OMB)
United States Trade Representative (USTR)

Executive Agencies
Department of Agriculture (USDA)
Department of Commerce (DOC)
Department of Defense (DOD)
Department of Education
Department of Energy
Department of Health and Human Services (HHS)
Department Homeland Security (DHS)
Department of Housing and Urban Development (HUD)
Department of the Interior (DOI)
Department of Justice (DOJ)
Department of Labor (DOL)
Department of State (DOS)
Department of Transportation (DOT)
Department of the Treasury
Department of Veterans Affairs

INDEPENDENT AGENCIES
Advisory Council on Historic Preservation (ACHP)
American Battle Monuments Commission
Central Intelligence Agency (CIA)
Commodity Futures Trading Commission (CFTC)
Consumer Product Safety Commission (CPSC)
Corporation for National Service
Environmental Protection Agency (EPA)
Equal Employment Opportunity Commission (EEOC)
Farm Credit Administration (FCA)
Federal Communications Commission (FCC)
Federal Deposit Insurance Corporation (FDIC)
Federal Election Commission (FEC)
Federal Energy Regulatory Commission (FERC)
Federal Labor Relations Authority (FLRA)
Federal Maritime Commission
Federal Reserve System, Board of Governors of the Federal Reserve System
Federal Retirement Thrift Investment Board (FRTIB)
Federal Trade Commission (FTC)
General Services Administration (GSA)
Federal Consumer Information Center (Pueblo, CO)
Institute of Museum and Library Services (IMLS)

International Boundary and Water Commission
International Broadcasting Bureau (IBB)
Merit Systems Protection Board (MSPB)
National Aeronautics and Space Administration (NASA)
National Archives and Records Administration (NARA)
National Capital Planning Commission (NCPC)
National Commission on Libraries and Information Science (NCLIS)
National Council on Disability
National Credit Union Administration (NCUA)
National Endowment for the Arts (NEA)
National Endowment for the Humanities (NEH)
National Indian Gaming Commission (NIGC)
National Labor Relations Board (NLRB)
National Mediation Board (NMB)
National Railroad Passenger Corporation (AMTRAK)
National Science Foundation (NSF) Board
National Transportation Safety Board (NTSB)
Nuclear Regulatory Commission (NRC)
US Nuclear Waste Technical Review Board (NWTRB)
Occupational Safety and Health Administration (OSHA)
Office of Federal Housing Enterprise Oversight (OFHEO)
Office of Personnel Management (OPM)
Overseas Private Investment Corporation (OPIC)
Peace Corps
Pension Benefit Guaranty Corporation
Postal Rate Commission
Railroad Retirement Board (RRB)
Securities and Exchange Commission (SEC)
Selective Service System (SSS)
Small Business Administration (SBA)
Social Security Administration (SSA)
Tennessee Valley Authority (TVA)
Thrift Savings Plan (TSP)
United States Agency for International Development (USAID)
United States Arms Control and Disarmament Agency (ACDA)
United States International Trade Commission (USITC)
United States Office of Government Ethics (OGE)
United States Postal Service (USPS)
United States Trade and Development Agency
Voice of America (VOA)

Attachment B: Identification of USG National Security Systems

- Computer Security Act of 1987: This Act clarified the definition of "national security-related information," and assigned the National Institute of Standards and Technology (NIST) the responsibility and authority of developing all Federal standards for safeguarding unclassified systems. The National Security Agency (NSA) was assigned responsibility for security of information that is classified for national security purposes.
- This definition was most recently included in the U.S. Federal Information System Management Act (FISMA) of 2002 (please see http://csrc.nist.gov/policies/FISMA-final.pdf), excerpted below:

2.0 Basis for Identification of National Security Systems

"(2)(A) The term 'national security system' means any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—

(i) the function, operation, or use of which-
(I) involves intelligence activities;
(II) involves cryptologic activities related to national security;
(III) involves command and control of military forces;
(IV) involves equipment that is an integral part of a weapon or weapons system; or
(V) subject to subparagraph (B), is critical to the direct fulfillment of military or intelligence missions; or
(ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

(B) Subparagraph (A)(i)(V) does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications)."

Systems not meeting any of these criteria are not national security systems.