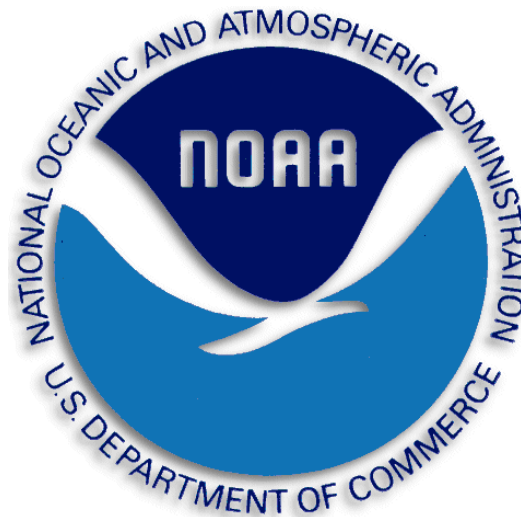


NOAA/NESDIS

Policy and Procedures for Ensuring Security in Acquisitions of NESDIS IT Systems and NESDIS Services

February 15, 2014



Prepared by:

**U.S. Department of Commerce
National Oceanic and Atmospheric Administration (NOAA)
National Environmental Satellite, Data, and Information Service (NESDIS)**

Table of Contents

Policy and Procedures for Ensuring Security in Acquisitions of NESDIS IT Systems and NESDIS Services	3
1.0 Background and Purpose	1
2.0 Scope	1
3.1 Roles, Responsibilities, and Coordination.....	1
3.2 System Owner (SO).....	1
3.3 Contracting Officer (CO)	1
3.4 Contracting Officer’s Representative (COR)	2
3.5 Assistant Chief Information Officer (ACIO)	2
3.6 Information System Security Officer (ISSO).....	2
3.7 Information Security Program Manager (ITSPM)	2
3.8 Information Technology Security Officer (ITSO).....	2
4.0 Management Commitment	2
5.1 Compliance.....	3
5.2 References.....	3
6.1 Policy	3
6.2 Policy Maintenance	3
6.3 Policy Feedback Process	4
6.4 Policy Effective Date	4
6.5 Procedures for Ensuring Security in NESDIS Acquisitions	4
7.2 Procedures for Development Contracts	5
7.2 Procedures for External Information System Services Contracts	8
7.3 IT Products Contracts	9
7.4 Applicable Commerce Acquisition Regulations for Service and IT Procurements.....	9
7.4 Checklist Signature Authorities.....	10
Appendix A Template for Security Requirements in Development Contracts	11
Appendix B: Template for Security Requirements in External Information System Services Contracts (including Cloud Providers)	14

Policy and Procedures for Ensuring Security in Acquisitions of NESDIS IT Systems and NESDIS Services

RECORD OF CHANGES/REVISIONS

Version	Date	Section	Author	Change Description
Draft 0.1d	10/2008	All	NESDIS ITSO	1 st Draft
Draft 0.2d	01/2009	All	NESDIS ITSO	Address initial IRMT Security Team comments.
Draft 0.3d	01/29/2010	3, 6.3, 7.4.4	NESDIS ITSO	Address 2 nd round of IRMT Security Team comments.
Draft 0.4d	07/14/2010	7.5, Appendix A	NESDIS ITSO	Add section on Checklist Delegation of Authority; remove Checklist as a separate document and attempt to simplify by referencing NESDIS SOW templates.
1.0	08/20/2010	All	NESDIS ITSO	Add use of DOC Checklist as acceptable alternative to NESDIS Checklist. Finalize and prepare for issuance
Draft 2.0	5/31/2012	All	NESDIS ITSO Support Staff	Biennial update
2.1	9/28/2012	All	NESDIS ITSO	Finalize and prepare for CIO issuance
3.0	10/15/2013		NESDIS ITSPM	Annual review and update
3.1	02/15/2014	Appendix A	NESDIS ITSPM	Updated for change of Supply Chain Risk legislation issued in January 2014

1.0 Background and Purpose

In accordance with the Federal Information Security Management Act (FISMA, Public Law 107-347), contractor access to government information or government information technology (IT) systems requires compliance with agency IT security policy. Aspects of the Department of Commerce (DOC) *IT Security Program Policy* (ITSP) apply in many situations, such as to personnel performing duties that require access to a DOC computer (from basic e-mail account on a DOC network to privileged system administrator access), to offsite services provided by a contractor for the storage or processing of DOC information on behalf of DOC. In addition, procurement of IT products such as hardware and software may require specifications for compliance with federal government policies such as the United States Government Configuration Baseline (USGCB), Homeland Security Presidential Directive (HSPD) 12 (August 2004), and the Office of Management and Budget Memorandum for Transition to Internet Protocol version 6 (September 2010).

The *Policy and Procedures for Ensuring Security in NESDIS IT Systems and Services Acquisitions* provides the method for implementing security in acquisitions as recommended by the National Institute of Standards and Technology (NIST) Special Publications (SP). This document shall satisfy the requirements for NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, control SA-1, *System and Services Acquisition Policy and Procedures*, within NESDIS.

2.0 Scope

All NESDIS employees and contractors with significant IT systems management, IT administration, information security, or IT roles for NESDIS that become involved with NESDIS system and services acquisitions.

3.1 Roles, Responsibilities, and Coordination

3.2 System Owner (SO)

The SO coordinates with the Contracting Officer (CO), the Contracting Officer's Representative (COR), their Information System Security Officer (ISSO), and NESDIS IT Security Officer (ITSO) to ensure that the acquisition team (1) completes an *Information Security in Acquisitions Checklist* (ISAC) and (2) submits the completed checklist with budgetary requests to the CO for inclusion in Statements of Work (SOW) and Requests for Proposal (RFP) or equivalent contract work performance document. The SO consults with the NESDIS ITSO as necessary to ensure the checklist is properly completed, and the SO signs the checklist.

3.3 Contracting Officer (CO)

The CO shall coordinate with the SO and COR to ensure receipt of a completed ISAC, and sign the ISAC prior to issuance of Requests for Bid and RFPs for NESDIS systems and services.

3.4 Contracting Officer's Representative (COR)

The COR shall coordinate with the SO and ISSO to complete an ISAC. The COR signs the ISAC to acknowledge their involvement in determining the responses and inclusion of the required IT security language in the SOW and RFP or equivalent contract work performance document.

3.5 Assistant Chief Information Officer (ACIO)

The NOAA Assistant Chief Information Officer (CIO) for Satellite and Information Services shall evaluate requests for Re-Delegation of Authority for ISSOs to sign the ISAC for the NESDIS ITSO (see section 7.5) and shall issue IT security-related policies.

3.6 Information System Security Officer (ISSO)

The ISSO shall coordinate with the COR and SO to ensure proper completion of the ISAC. The ISSO consults with the NESDIS ITSO as necessary to ensure accuracy in completing the ISAC. The ISSO signs the ISAC to acknowledge their involvement in determining the responses. Federal ISSOs may apply for a Re-Delegation of Authority to sign the checklist on behalf of the ITSO (see section). To eliminate any appearance of conflict of interest, the contractor ISSOs are not eligible for the Re-Delegation of Authority.

3.7 Information Security Program Manager (ITSPM)

The NESDIS ITSPM oversees the activities of the ITSO and manages the NESDIS IT Security Program. The ITSPM maintains the NESDIS IT security policies and procedures and has authority to sign the ISAC on behalf of the ITSO for procurements valued up to \$10 million.

3.8 Information Technology Security Officer (ITSO)

The NESDIS ITSO, or the Alternate ITSO, shall support the ITSPM in executing this policy and procedures and shall advise the SO, ISSO, and COR to ensure the adequacy of security requirements in procurements and the accuracy of responses on the ISAC and will sign the ISAC to indicate their involvement in determining the responses.

4.0 Management Commitment

The NESDIS Chief Information Division (CID) supports the NESDIS Assistant Administrator's (AA) strong emphasis on securing NESDIS information and information systems. Through the issuance of this policy and accompanying procedures, it demonstrates this commitment for ensuring security in NESDIS systems and services acquisition practices.

5.1 Compliance

The NESDIS ITSPM shall review NESDIS acquisition documents periodically for compliance with this policy and accompanying procedures. COs and CORs of acquisitions found not in compliance with this policy will be reported to the National Oceanic and Atmospheric Administration (NOAA) Procurement Executive for disciplinary action such as removal of acquisition authority. SOs, as well as ISSOs and the NESDIS ITSO, found not in compliance with this policy will be reported to their Office Director or the system Authorizing Official, as appropriate, with a recommendation for administrative action including removal from acquisition-related responsibilities.

5.2 References

- DOC *Information Technology Security Program Policy* (ITSP), section 4.15.
- Commerce Acquisition Manual 1337.70, *Personnel Security Requirements*
- NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, in the System and Services Acquisition (SA) family of controls, specifies the requirements for documenting inclusion of security in acquisitions.
- NIST SP 800-64, Revision 2, *Security Considerations in the Information System Development Life Cycle* (SDLC), Appendix F, provides acquisition planning considerations that contribute to information security during the Development / Acquisition phase of the SDLC.

6.1 Policy

As required by DOC ITSP section 4.15, all NESDIS services and IT systems acquisition documentation shall include the DOC/NESDIS ISAC and security specifications, either explicitly or by reference, in information systems and services acquisition contracts based on an assessment of risk and in accordance with applicable laws, Executive Orders, directives, policies, regulations, and standards. The ISAC template can be found on the NESDIS IT Security Handbook website at https://intranet.nesdis.noaa.gov/ocio/it_security/handbook/it_security_handbook.php. The NESDIS CIO requires all NESDIS Security Controls Assessors to assess the completeness and accuracy of the ISAC in years when the SA-4 control is selected for security controls assessment (at least once every 3 years).

6.2 Policy Maintenance

The NESDIS ITSO shall review this policy and procedures annually and update as necessary to reflect implementation challenges and new requirements. All updates to the policy and procedures shall be subject to a NESDIS-wide vetting process providing an opportunity for stakeholders to comment on the programmatic implications of updates. Policy updates shall be issued by the NESDIS ACIO.

6.3 Policy Feedback Process

NESDIS personnel are encouraged to notify the ITSO via e-mail at nesdis.it.security@noaa.gov regarding any errors found in the document or other clarifications or updates that are required.

6.4 Policy Effective Date

This policy is effective within 30 days of issuance. After this 30-day grace period, acquisitions for new IT systems, components, products, and services must fully comply with the NESDIS policy and procedures.

6.5 Procedures for Ensuring Security in NESDIS Acquisitions

In accordance with the following procedures and the references in section 5.1, SOs must complete the *DOC/NESDIS Information Security in Acquisitions Checklist* (available on the NESDIS IT Security Handbook website at https://intranet.nesdis.noaa.gov/ocio/it_security/handbook/it_security_handbook.php) prior to issuing a RFP or SOW for acquisition of

- **all** NESDIS services (IT or non-IT), including procurements of IT system development services, above the \$3,000 micro-purchase threshold, and
- **all** IT products (hardware and software), regardless of value.

NESDIS has supplemented and clarified the DOC ISAC content for use within NESDIS for acquisition of services and IT systems and products. The following requirements for ensuring security in acquisitions must be met in the documentation for NESDIS procurements meeting the above criteria.

- Indicate the NOAA system ID (on pages 1 and 3) that governs the IT security policy for the service or product acquisition.
- Indicate the nature of the acquisition on the checklist as well as the RFP or solicitation number (on page 3).
- Indicate the security category of the system that the acquisition supports (on page 3).
- The ISAC shall be completed before issuing requests for proposals for systems and services acquisitions in order to determine whether the product or service to be acquired will require additional considerations for security requirements, and to ensure that the solicitation includes these requirements before requesting vendor bids. In order to successfully complete this checklist, each question should be addressed in coordination with all members of the Acquisition Team including: the Procurement Requestor from the Program Office (SO or program manager), the COR, Information System Security Officer (ISSO) and staff from the NESDIS Division/Office initiating the procurement, the ITSO, and the Contracting Official from the NESDIS servicing Acquisition Office.

- With the renewed emphasis on trustworthy information systems and supply chain security, it is essential that organizations have the capability to express their information security requirements with clarity and specificity in order to engage the information technology industry and obtain the systems, components, and services necessary for mission and business success. In addition to completing the DOC/NESDIS ISAC, the practices recommended by NIST SP 800-53, Revision 4 in controls SA-4, SA-5, SA-8, SA-9, SA-10, and SA-11, shall be implemented within NESDIS for acquisitions supporting systems categorized as Moderate and High security impact and in controls SA-12, SA-15, SA-16, SA-17 for systems categorized as High security impact. NESDIS solicitation documents (e.g., Requests for Proposals) for information systems and services must permit updating security control requirements as new threats/vulnerabilities are identified and as new technologies are implemented. Standardized IT security minimum language templates are provided on the IT Security Handbook website at https://intranet.nesdis.noaa.gov/ocio/it_security/handbook/it_security_handbook.php. At a minimum, security considerations in SOWs must address personnel security and compliance with the DOC ITSPP as applicable to the nature of the work; and, development or external information service support contracts must contain, as applicable, the following minimum elements:

7.2 Procedures for Development Contracts

See [Appendix A](#) for the Development Contract Template. Development contracts must address:

- 7.1.1 **Security functional requirements/specifications:** Require developers to build specific security controls – as recommended by the revision of NIST SP 800-53 currently in effect (e.g., as of August 2011, Revision 3 is in effect and in April 2014 Revision 4 is in effect) – into the system/component at the level required by the system’s FIPS 199 security categorization (i.e., high, moderate, or low).
- 7.1.2 **Developmental and evaluation-related assurance requirements:** Require developers to apply security engineering principles (control SA-8), follow a configuration management process (control SA-10), and perform security testing and evaluation (control SA-11) before delivery to the government.
- 7.1.3 **Security-related documentation requirements:** Developers must provide the government with adequate documentation of the system/component developed, to include a narrative description of the system operating environment, architecture (including diagrams and hardware/software inventories), configuration settings and implementation manuals, and user/operator manuals (control SA-5). The solicitation documents include requirements for appropriate information system documentation. The documentation addresses user and systems administrator guidance and information regarding the implementation of the security controls in the information system. The level of detail required in the documentation is based on the FIPS 199 security category for the information system.

- 7.1.4 **Use of Tested, Evaluated, and Validated Products:** NIST SP 800-23 provides guidance on the acquisition and use of tested/evaluated information technology products. NIST SP 800-36 provides guidance on the selection of information security products. This requirement supports Trustworthiness (control SA-13 if applicable to the system under development).
- 7.1.5 **Configuration Settings and Implementation Guidance:** The contractor must build components using the IT standards and settings as specified by the Government. OMB’s FISMA reporting instructions provide guidance on configuration requirements for federal information systems. NIST provides requirements for compliance with the U.S. Government Configuration Baseline requirements for some Microsoft Windows products, and NIST SP 800-70 provides guidance on configuration settings for other information technology products.
- 7.1.6 **Software Development:** If applicable to the contract, custom software shall be developed and tested in accordance with the Department of Homeland Security’s (DHS) *Build Security In* best practices (online at <https://buildsecurityin.us-cert.gov/>). Software shall be resilient across the development, acquisition, and operational lifecycle; as such, Software Assurance practices must address trustworthiness, dependability (correct and predictable execution), conformance, and survivability. DHS Pocket Guides for software assurance best practices and acquisition considerations are available online at <https://buildsecurityin.us-cert.gov/swa/software-assurance-pocket-guide-series/>. This may be described in conjunction with the *Development Process, Standards, and Tools* section (section 7.1.7.2 below) for high-impact system software.
- 7.1.7 Additional Requirements for Developers of High-impact systems and components (NOTE: replace the yellow-highlighted “high” text with “moderate” if used for a moderate system):
- 7.1.7.1 **Supply Chain Protection** (control SA-12): Developers of high-impact system components must implement a process consistent with the requirements of the *National Strategy for Global Supply Chain Security* (online at http://www.whitehouse.gov/sites/default/files/national_strategy_for_global_supply_chain_security.pdf).
- 7.1.7.2 **Development Process, Standards, and Tools** (control SA-15): Developers must follow a documented development process that:
- Explicitly addresses security requirements;
 - Identifies the standards and tools used in the development process (for example, programming languages and computer-aided design (CAD) systems);
 - Documents the specific tool options and tool configurations used in the

development process; and

- Documents, manages, and ensures the integrity of changes to the process and/or tools used in development to enable accurate supply chain risk assessment and mitigation, and require robust configuration control throughout the life cycle (including design, development, transport, delivery, integration, and maintenance) to track authorized changes and prevent unauthorized changes; and
- Permits the Government to review the developer's process, standards, tools, and tool options/configurations as part of the source selection evaluation to determine if the process, standards, tools, and tool options/configurations selected and employed can satisfy the requirements for a high-impact system test and development environment (for example, the use of maturity models to determine the potential effectiveness of such processes).

7.1.7.3 **Developer-Provided Training** (control SA-16): Developers must provide training on the correct use and operation of the implemented security functions, controls, and/or mechanisms. Training of personnel is an essential element to ensure the effectiveness of security controls implemented within organizational information systems. Training may be classroom-style training, web-based/computer-based training, or hands-on training. The contractor must also provide sufficient training materials for the government to conduct in-house training or offer self-training to organizational personnel after initial system deployment.

7.1.7.4 **Developer Security Architecture and Design** (control SA-17): Developers must produce a design specification and security architecture that:

- Is consistent with and supportive of the high-impact security architecture to demonstrate consistency with the NESDIS enterprise architecture and information security architecture;
- Accurately and completely describes the required security functionality, and the allocation of security controls among physical and logical components; and
- Expresses how individual security functions, mechanisms, and services work together to provide required high-impact security capabilities and a unified approach to protection.

7.2 Procedures for External Information System Services Contracts

External information system services contracts require that providers comply with specific organizational information security requirements (i.e., the DOC ITSPP) and activities (control SA-9). These contracts also require that providers employ appropriate security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance (i.e., NIST SP 800-53). The providers must identify the functions,

ports, protocols, and other services required for the use of such services. NIST SP 800-35 provides guidance on information technology security services. Organizations must consult the Federal Risk and Authorization Management Program (FedRAMP) when acquiring cloud services from external providers. FedRAMP addresses required security controls and independent assessments for a variety of cloud services. Additional information is available at <http://www.fedramp.gov>. See [Appendix B](#) for a recommended template for contract statements of work.

7.3 IT Products Contracts

Acquisition and development of information technology components and systems shall adhere to the requirements of H.R. 933, DIVISION B—*COMMERCE, JUSTICE, SCIENCE, AND RELATED AGENCIES APPROPRIATIONS ACT, 2013*, Title V, Section 516 (online at <http://www.gpo.gov/fdsys/pkg/BILLS-113hr933enr/pdf/BILLS-113hr933enr.pdf>).

7.4 Applicable Commerce Acquisition Regulations for Service and IT Procurements

See the NESDIS IT Security Handbook website at https://intranet.nesdis.noaa.gov/ocio/it_security/handbook/it_security_handbook.php for security requirement templates using these CARs as indicated by the responses determined in completion of the ISAC. Depending on the nature of the work described in the statement of work, if personnel require access to DOC/NOAA facilities or IT equipment, one or more of the following Commerce Acquisition Regulations (CARs) must be included in the statement of work, as appropriate:

- CAR 1352.237-70, *Security processing requirements—high or moderate risk contracts*
- CAR 1352.237-71, *Security processing requirements—low risk*
- CAR 1352.237-72, *Security processing requirements—national security contracts*
- CAR 1352.237-73, *Foreign national visitor and guest access to departmental resources*
- CAR 1352.239-72, *Security requirements for information technology resources*

To determine which of the security processing CARs to include in the contract, refer to the Commerce Acquisition Manual (CAM) 1337.70, *Department of Commerce Personnel Security Requirements*, for the criteria to determine whether the contract is non-IT- or IT-related, whether high, moderate, or low IT or non-IT risk, or whether national security-related (online at https://max.omb.gov/community/download/attachments/584123646/CAM_1337-700_Personnel_Security_Requirements.pdf?version=1&modificationDate=1312833819495).

For the Federal Acquisition Regulation (FAR) Title 48, Part 1337, *Service Contracting*, provisions go online to <http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&SID=1dc767c899eab4c6f41a7162dc872adc&rgn=div5&view=text&node=48:5.0.6.48.34&idno=48>.

For the FAR Title 48, Part 1339, *Acquisition of Information Technology*, provisions go online to <http://www.ecfr.gov/cgi-bin/text->

[idx?c=ecfr&sid=ba6274cadd0fbbb589202282915b97f3&rgn=div5&view=text&node=48:5.0.6.48.35&idno=48](http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&sid=ba6274cadd0fbbb589202282915b97f3&rgn=div5&view=text&node=48:5.0.6.48.35&idno=48)).

Go to the FAR Title 48, Part 1352-2, *Text of Provisions and Clauses*, to find the full text of the CARs cited in the FAR and the ISAC (online at http://www.ecfr.gov/cgi-bin/text-idx?SID=1dc767c899eab4c6f41a7162dc872adc&c=ecfr&tpl=/ecfrbrowse/Title48/48cfrv5_02.tpl#1300).

7.4 Checklist Signature Authorities

All procurements for NESDIS services above the micro-purchase threshold of \$3,000 and all procurements for IT-related acquisitions for hardware and software (regardless of value) must be submitted to the NESDIS CID for review and approval of the ISAC. The NESDIS IT Security Program Manager, NESDIS ITSO, and NESDIS Alternate ITSO have signature authority for procurements up to a threshold of \$10 million total contract value. The NESDIS CID personnel shall have 2 business days to process the procurement package and either sign the ISAC or return the package with recommendations for improving the security requirements. For procurements with a total contract value above \$10 million, the ISAC must also be signed by the NOAA IT Security Director or NOAA ITSO must also be obtained on the ISAC.

The Checklist may be signed either manually or using a digital signature.

In addition, on March 20, 2007, the NOAA CIO issued a memorandum delegating signature authority for the ISAC to Line Office CIOs for all contracts that involve IT-related services up to \$10M. On June 15, 2007, the NOAA CIO issued a memorandum that clarified the delegation authority to Line Office CIOs, their deputies, and their ITSOs. The memo also permits Line Office CIOs to re-delegate their delegated signature authority for the ISAC to federal ISSOs. The re-delegation gives the ISSO the authority to sign ISACs for all services acquisitions up to \$500,000 that are not for developing new information systems. ISACs for services acquisitions that do not meet these criteria must be forwarded to the NESDIS CID for review and signature by the IT Security Program Manager, ITSO, or Alternate ITSO. In order to receive this re-delegated authority, an ISSO must first complete the required e-learning course, *Effectively Integrating Information Technology (IT) Security into the Acquisition Process* (available on-line at <https://max.omb.gov/community/display/DOC/IT+Security+in+the+Acquisition+Process>). Upon completion of the course, the ISSO must provide a copy of the completion certificate to the NESDIS ITSO. Within 15 business days, the CIO will issue a letter of re-delegation of authority to the ISSO and provide a copy to the SO, the NOAA Office of the CIO, and the NOAA Acquisition and Grants Office.

Appendix A Template for Security Requirements in Development Contracts

[Select and modify applicable suggested text, and insert into SOW. Yellow-highlighted areas require customization or additional details pertaining to the IT procurement.]

Security functional requirements/specifications. Developers shall build specific security controls—as specified by the Government and based on the recommendations of the most recent revision of NIST Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*—into the system/component at the level required by the system’s FIPS 199 security categorization as determined by the Government to be **[select: high, moderate, or low]**.

- System components shall permit updating security controls as new threats/vulnerabilities are identified and as new technologies are implemented.
- Acquisition and development of information technology components and systems shall adhere to the requirements of H.R. 3547, DIVISION B—*COMMERCE, JUSTICE, SCIENCE, AND RELATED AGENCIES APPROPRIATIONS ACT, 2014*, Title V, Section 515.

Developmental and evaluation-related assurance requirements. Developers shall follow security engineering principles (including secure coding practices and code review for software development) consistent with NIST SP 800-27, *Engineering Principles for Information Technology Security (A Baseline for Achieving Security)*, to follow a configuration management process in accordance with NIST SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems*, and to perform security testing and evaluation before delivery to the government, specifically, developer/contractors shall:

- Create and implement a Configuration Management Plan;
- Create and implement a security test and evaluation plan;
- Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process; and
- Document the results of the security testing/evaluation and flaw remediation processes in a Security Test and Evaluation Plan, Requirement, Objectives, and Results Report.

Use of Tested, Evaluated, and Validated Products: Developers shall, to the extent technically possible, incorporate products that have been tested, evaluated, and validated by the government. NIST SP 800-23, *Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products*, provides guidance on the acquisition and use of tested/evaluated information technology products. NIST SP 800-36, *Guide to Selecting Information Technology Security Products*, provides guidance on the selection of information security products.

Security-related documentation requirements. Developers shall provide the government with adequate documentation of the system/component developed, to include a narrative description of the system operating environment, architecture (including diagrams and hardware/software inventories), and user/operator manuals. The documentation shall address user and systems administrator guidance and

information regarding the implementation of the security controls in the information system. The documentation shall include, but is not limited to:

- Vendor supplied documentation of software;
- Supporting narratives as required by the government to prepare a comprehensive system security plan;
- Standard operating procedures;
- Emergency procedures;
- User rules/procedures
- User and Administrator manuals; and
- Backup procedures.

Configuration Settings and Implementation Guidance: [Describe the information system requirements for security configuration settings and security implementation procedures. List all mandated settings here that pertain to components under the contract.] The information system requirements include security configuration settings and security implementation guidance, specifically:

- U.S. Government Configuration Baseline (USGCB): NIST provides requirements for compliance requirements for some Microsoft Windows products at <http://usgcb.nist.gov/>, and
- NIST SP 800-70, *National Checklist Program for IT Products--Guidelines for Checklist Users and Developers* and the National Vulnerability Database (<http://web.nvd.nist.gov/view/ncp/repository>) provide guidance on selecting secure configuration settings for other information technology products. For this system, the following secure benchmarks are required:

CIS for Operating System X

DISA STIG for Operating System Y

Etc.

Software Development: Software shall be developed and tested in accordance with the Department of Homeland Security's *Build Security In* best practices (online at <https://buildsecurityin.us-cert.gov/>). Software shall be resilient across the development, acquisition, and operational lifecycle; as such, Software Assurance practices must address trustworthiness, dependability (correct and predictable execution), conformance, and survivability.

Development Process, Standards, and Tools: [NOTE: Required for High-impact systems; optional for Moderate systems] The developer shall follow a documented development process that:

- Explicitly addresses security requirements;

- Identifies the standards and tools used in the development process (for example, programming languages and computer-aided design (CAD) systems);
- Documents the specific tool options and tool configurations used in the development process; and
- Documents, manages, and ensures the integrity of changes to the process and/or tools used in development to enable accurate supply chain risk assessment and mitigation, and require robust configuration control throughout the life cycle (including design, development, transport, delivery, integration, and maintenance) to track authorized changes and prevent unauthorized changes; and
- The Government shall review the developer's process, standards, tools, and tool options/configurations as part of the source selection evaluation to determine if the process, standards, tools, and tool options/configurations selected and employed can satisfy the requirements for a high-impact system test and development environment (for example, the use of maturity models to determine the potential effectiveness of such processes).

Developer-Provided Training: [NOTE: Required for High-impact systems; optional for Moderate systems] The developer shall provide [*select: user-level, system administrator, other training*] on the correct use and operation of the implemented security functions, controls, and/or mechanisms. Training of personnel is an essential element to ensure the effectiveness of security controls implemented within organizational information systems. Training must be [*select: classroom-style training, web-based/computer-based training, and hands-on training*]. The contractor must also provide sufficient training materials for the government to conduct in-house training or offer self-training to organizational personnel after initial system deployment.

Security Architecture and Design: [NOTE: Required for High-impact systems; optional for Moderate systems] The Contractor shall produce a design specification and security architecture that:

- Is consistent with and supportive of the **high**-impact security architecture to demonstrate consistency with the NESDIS enterprise architecture and information security architecture;
- Accurately and completely describes the required security functionality, and the allocation of security controls among physical and logical components; and
- Expresses how individual security functions, mechanisms, and services work together to provide required **high**-impact security capabilities and a unified approach to protection.

Appendix B: Template for Security Requirements in External Information System Services Contracts (including Cloud Providers)

The Contractor shall comply with specific organizational information security requirements and activities as specified in CAR 1352.239-72, *Security Requirements For Information Technology Resources* (April 2010), including development of a Security Authorization Package as required by CAR 1352.239-72, section (i). The Contractor may provide evidence of security authorization to operate granted under the Federal Risk and Authorization Management Program (FedRAMP). FedRAMP addresses required security controls and independent assessments for a variety of cloud services. Additional information is available at <http://www.fedramp.gov>.

The Contractor shall employ appropriate security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance—as specified by the Government and based on the recommendations of the most recent revision of NIST Special Publication (SP) 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*—into the system/component at the level required by the system’s FIPS 199 security categorization as determined by the Government to be **[select: high, moderate, or low]**.

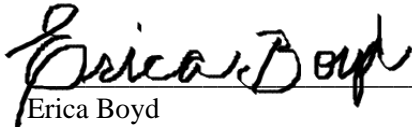
The Contractor shall identify for Government acceptance the functions, ports, protocols, and other services required for the use of the external information services. **Insert details specific to the system supported by this contract.**

[Refer to NIST SP 800-35, Guide to Information Technology Security Services, for guidance on information technology security services and what to consider for inclusion in the SOW.]

Approval Page

Document Number: NQP-3412, Revision 3.2	
Document Title Block: Policy and Procedures for Ensuring Security in Acquisitions of NESDIS IT Systems and NESDIS Services	
Process Owner: NESDIS Chief Information Division	Document Release Date: February 15, 2014

Prepared by:



Erica Boyd
Ambit- Associate Consultant
NESDIS Chief Information Office

3/26/15

Date:

Approved by:



Irene Parker
Assistant Chief Information Officer - Satellites

3/26/15

Date:

Document Change Record

VERSION	DATE	CCR #	SECTIONS AFFECTED	DESCRIPTION
3.2	March 26, 2015	----	ALL	Baseline NQP-3412