

NESDIS

Policy and Procedures for Determining Minimum Documentation Requirements for System Interconnections

September xx, 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

NESDIS Policy and Procedures for Determining Minimum Documentation Requirements for System Interconnections.....	6
Record of Changes/Revisions.....	6
1.0 Background and Purpose	1
2.0 Scope.....	1
3.1 Roles, Responsibilities, and Coordination	1
3.3 Information Owner (IO)	2
3.4 Authorizing Official (AO)	2
3.5 Information System Security Officer (ISSO)	2
3.6 Information Technology Security Officer (ITSO)	2
4.0 Management Commitment	2
5.1 Compliance	2
5.2 References	3
6.1 NESDIS Policy	3
6.2 Policy Maintenance.....	3
6.3 Policy Feedback Process	3
6.4 Policy Effective Date	4
7.1 Documentation Procedures	4
7.2 Documentation Requirement Types.....	4
7.2.2 Service Level Agreement (SLA)	5
7.2.3 Interconnection Security Agreement (ISA).....	5
7.2.4 Memorandum of Understanding (or Agreement) (MOU/A)	5
7.2.5 Variances	5
7.3 Interconnection Types and Purpose	6
7.3.2 NESDIS-to-NOAA	6
7.3.3 NESDIS-to-Government, Non-NOAA	7
7.3.4 NESDIS-to-Academia/Scientific Community.....	7
7.3.5 NESDIS-to-International	7
7.3.6 NESDIS-to-Commercial Communications Service Provider	8
7.3.7 NESDIS-to-Other.....	8

7.4 Determining Documentation Requirements.....	8
Appendix A: Technical Security Language Matrix for International Agreements	12
Appendix B: ISA Creation Workflow	16



**UNITED STATES DEPARTMENT OF
COMMERCE**
National Oceanic and Atmospheric
Administration
NATIONAL ENVIRONMENTAL SATELLITE
DATA AND INFORMATION SERVICE
Silver Spring, Maryland 20910

September 30, 2012

MEMORANDUM FOR: Distribution

FROM: Catrina D. Purvis 
NESDIS Chief Information Officer (Acting)

SUBJECT: Issuance of Updated NESDIS Information Technology
Security Policies and Procedures

This is to announce the issuance of ten updated NESDIS publications for implementing effective, compliant, and consistent information technology (IT) security practices within NESDIS. These documents highlight the specific steps necessary to ensure effective NESDIS implementation. Specifically issued under this memorandum are the

1. NESDIS *Federal Information Processing Standard 199 Security Categorization Policy and Procedures*, v3.0;
2. NESDIS *Plan of Action and Milestones Management Policy and Procedures*, v2.0;
3. NESDIS *Policy and Procedures for Determining Minimum Documentation Requirements for System/IT Interconnections*, v2.1;
4. NESDIS *Contingency Planning Policy and Procedures*, v2.1;
5. NESDIS *Policy and Procedures for Ensuring Security in NESDIS IT Systems and Services Acquisitions*, v2.1;
6. NESDIS *Security Assessment Report Policy and Procedures*, v2.0;
7. NESDIS *Federal Information Security Management Act (FISMA) Inventory Management Policy and Procedures*, v2.0;
8. NESDIS *IT Security Training Policy and Procedures*, v2.1;
9. NESDIS *Continuous Monitoring Planning Policy and Procedures*, v2.1; and the
10. *Practices for Securing Open-source Project for a Network Data Access Protocol Server Software on NESDIS Information Systems*, v3.1.

These publications are part of the NESDIS-wide effort to maintain and enhance its foundation of NESDIS IT security policies and implementation practices that align with the latest Department of Commerce and NOAA policies, requirements, and standards. I wish to thank all who contributed reviewing and commenting on the drafts prior to publication to ensure that they are complete, current, and meaningful. These documents will be posted to the Chief Information Division's Web site at https://intranet.nesdis.noaa.gov/ocio/it_security/handbook/itsecurityhandbook.php. If you have any questions, please contact the NESDIS IT Security Officer, Nancy DeFrancesco, at Nancy.DeFrancesco@noaa.gov or phone (301) 713-1312.

NESDIS Policy and Procedures for Determining Minimum Documentation Requirements for System Interconnections

Record of Changes/Revisions

Version	Date	Section	Author	Change Description
Draft 1.0	3/6/09	N/A	Noblis	Draft Submission for ITSO Review
Draft 1.1	6/15/09	All	Noblis	Updated based on IRMT and GC comments.
Draft 1.2	8/15/2009	All	N.DeFrancesco	Update and issue final for NESDIS-wide comment.
Final 1.0	8/31/2009	6.0	N.DeFrancesco	Address comments on final draft and finalize for CIO issuance.
Draft 2.0	3/29/12	All	A.Kuhn	Biennial Update
2.1 Final	9/28/2012	All	N.DeFrancesco	Finalize and prepare for CIO issuance

1.0 Background and Purpose

The Federal Information Security Management Act ([FISMA], 44 U.S.C. § 3541, *et seq.*), and the Office of Management and Budget (OMB) Circular A-130 Appendix III require management authorization (accreditation) of all information systems that store, process, or transmit federal data. Additionally, prior to interconnecting a system with other systems, OMB A-130 Appendix III requires that management provide written authorization based upon its review and acceptance of risk to the system.

The Department of Commerce *Information Technology Security Program Policy* (ITSPP) requires compliance with National Institute of Standards and Technology (NIST) guidance, specifically NIST Special Publication (SP) 800-47, *Security Guide for Interconnecting Information Technology Systems*, for documenting system interconnections. NIST SP 800-47 provides detailed guidance on how to develop the various documents which must be submitted to authorize an interconnection. It provides emphasis on interconnections between two or more information systems that are owned or operated by different organizations. NIST SP 800-47, however, does not provide guidance on how to determine which documents are required for requesting management’s authorization of an interconnection. It also does not address what documents are required for obtaining management’s authorization for interconnecting systems owned or operated by the same organization.

The Department of Commerce *Agreements Handbook* promotes “uniform implementation of interagency and other agreements throughout the Department, while giving due consideration to different individual program requirements and procedures.”

The purpose of this National Environmental Satellite, Data, and Information Service (NESDIS) policy and procedures document is to assist the System Owner (SO) with determining which of the interconnection documents are required for requesting management’s authorization for system interconnections, both internal and external.

2.0 Scope

The scope of this document is limited to identifying the minimum set of documents required for requesting that management authorize any system interconnection to/from NESDIS-owned or –operated information systems (including NESDIS-owned, contractor-operated information systems).

This document does not provide guidance on how to develop the required interconnection documents (e.g., Memorandum of Understanding/Agreement [MOU/A]) or Interconnection Security Agreement [ISA], etc). Such guidance is provided in NIST SP 800-47.

3.1 Roles, Responsibilities, and Coordination

3.2 System Owner (SO)

The SO is responsible for documenting and maintaining the terms and conditions for sharing data and information resources in a secure manner. The SO ensures the documentation is up-to-date and accurately reflects the interconnections between their system of responsibility and another system(s). If authorized by the Authorizing Official (AO), the SO can approve interconnections for development and test.

3.3 Information Owner (IO)

The IO (agency official with responsibility for establishing the controls for generation, collection, processing, dissemination, and disposal of the information) is responsible for communicating to the SO any limitations and/or condition(s) for the sharing of the information under their protection.

3.4 Authorizing Official (AO)

The AO is responsible for authorizing the interconnection and for accepting the risk associated with the interconnection.

3.5 Information System Security Officer (ISSO)

The ISSO is responsible for the development and maintenance of the security requirements documented in the ISA/MOU/A/Service Level Agreement (SLA).

3.6 Information Technology Security Officer (ITSO)

The NESDIS ITSO will advise the AO, SO, and the ISSO to ensure consistency and completeness of the agreements across the organization.

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 procedures, the CID demonstrates its commitment to ensuring that documentation submitted to request management authorization of system interconnections provides sufficient basis for a fully informed risk acceptance decision.

5.1 Compliance

The NESDIS ITSO monitors – through periodic quality reviews – documentation of interconnection security agreements within NESDIS to ensure compliance with applicable laws, directives, policies, and guidance. The ITSO reports to the AA monthly, and to the CIO and Office Directors as necessary regarding compliance. The AA, CIO, and/or Office Directors may initiate actions as necessary to correct reported deficiencies, including

reallocation of resources to improve implementation of security practices, or removal of an individual from their role as AO, SO, ITSO, or ISSO.

5.2 References

- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*
- NIST SP 800-53A, Revision 1, *Recommended Security Controls for Federal Information Systems and Organizations*
- NIST SP 800-47, *Security Guide for Interconnecting Information Technology Systems*
- NIST SP 800-64, *Security Considerations in the Information System Development Life Cycle.*
- NIST SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems*
- Office of Management and Budget Circular A-130, *Management of Federal Information Resources*, Appendix III, *Security of Federal Information Resources*
- Department of Commerce (DOC) *Information Technology Security Program Policy (ITSPP)*
- NOAA *IT Security Manual 212-1300*
- NESDIS *IT Security Handbook*

6.1 NESDIS Policy

As required by DOC ITSPP section 4.4.3, the NESDIS-specific ISA process and procedures shall align with the NIST SP 800-47 prescribed practices for the determining the security categorization of systems. This document provides NESDIS-specific procedures for determining the ISA documentation requirements and should be used as companion document to DOC and NOAA policies for implementation within NESDIS and not as a replacement document.

6.2 Policy Maintenance

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

6.3 Policy Feedback Process

NESDIS personnel are encouraged to notify the ITSO by e-mail to 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 upon issuance.

7.1 Documentation Procedures

NIST SP 800-47 defines an interconnection as the “direct connection of two or more Information Technology (IT) systems for the purpose of sharing data and other information resources.” NIST SP 800-47 focuses its guidance on system interconnections between different organizations. However, interconnections between systems within the same organization may also require detailed interconnection documentation to ensure data is protected and services are provided as agreed. Table 1 identifies the minimum set of documentation needed for management (i.e., AO) authorization.

Section 7.1 of this document provides a description of each type of interconnection documentation requirement identified in the Table 1 matrix.

Section 7.2 of this guide provides a description of each system interconnection type and purpose identified in the Table 1 matrix. These are descriptions of common types/purposes of NESDIS system interconnections and are provided to assist the SO in determining which connection type/purpose best describes the system interconnection for which authorization is being requested.

7.2 Documentation Requirement Types

7.2.1 System Security Plan (SSP)

The SSP is the primary document for describing the security of an information system. NIST SP 800-18 defines the SSP format used within NESDIS.¹ All system interconnections must be documented in section 11 of the SSP regardless of the type or purpose of the system interconnection. Each interconnection must be described in this section. The description should include an overview of the interconnection, and a summary of the interconnection agreement. The SSP must document all interconnection details.

7.2.2 Service Level Agreement (SLA)

A SLA is used to document what services the system will provide to other information systems. It should also document the expected confidentiality, integrity, and availability of the services provided. A SLA is typically used to document an interconnection where one system is dependent on the other, but not vice versa. A SLA is typically a provider to the customer document that contains provider directed contract information. It is usually not customized to the individual customer.

7.2.3 Interconnection Security Agreement (ISA)

An ISA is “a security document that specifies the technical and security requirements for establishing, operating, and maintaining the interconnection. It also supports the Memorandum of Understanding/Agreement between the two organizations. Specifically, the ISA documents the requirements for connecting the IT systems, describes the security controls that will be used to protect the system and data, contains a topological drawing of the interconnection, and provides a signature line.”² An ISA is a customized document between two parties.³

7.2.4 Memorandum of Understanding (or Agreement) (MOU/A)

The MOU/A documents the terms and conditions for sharing data and information resources in a secure manner. Specifically, the MOU/A defines the purpose of the interconnection; identifies relevant authorities; specifies the responsibilities of both organizations; and defines the terms of agreement, including the apportionment of costs and the timeline for terminating or reauthorizing the interconnection. The MOU/A should not include the technical details on how the interconnection is established or maintained; that is the function of the ISA.⁴

7.2.5 Variances

In more extensive international interconnection agreements, the format of each of the above document requirements may vary. This should be acceptable as long as the required topics are addressed. Any variation of the above document types however, must be coordinated with the ITSO and the AO for approval. Variations are considered control tailoring of NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*, Control CA-3 (*Information System Connection*) and should be documented appropriately and approved by the AO.

7.3 Interconnection Types and Purpose

7.3.1 NESDIS-to-NESDIS

A NESDIS-to-NESDIS interconnection is any NESDIS information system that interconnects with or shares information with another NESDIS information system. A NESDIS information system is defined as any information system identified with the NOAA5xxx numbering. NESDIS systems interconnect with other NESDIS systems for network/Internet connectivity, data sharing, or security services sharing. A NESDIS system interconnection can be a physical and logical connection. Since NESDIS-to-NESDIS systems share a common AO, interconnections for network/Internet connectivity and data sharing only require the interconnection to be documented in section 11 of the SSP. The AO's approval of the SSP constitutes acceptance of the interconnection.

NESDIS-to-NESDIS interconnections in which security services are utilized (i.e., common controls) should be documented in either an SLA or an ISA. A SLA is required where one system provides security services to a number of different systems. The SLA documents the expected services and level of confidentiality, integrity, and availability provided to all systems. For example, a NESDIS system providing audit log consolidation and management for all systems within the NOAA Satellite Operations Facility would create an SLA documenting the services offered, availability of those services, and the confidentiality and integrity of the data collected. A NESDIS system wishing to utilize the audit log services may do so by accepting the terms of the SLA. The SLA would provide a blanket interconnection document from one system to many systems. The ISA would be required where there is a single interconnection between two systems for shared security services or where the service is customized for an individual system.

7.3.2 NESDIS-to-NOAA

Most NESDIS systems have an interconnection (communications path provided) with a NOAA system for Internet connectivity and shared security services. For these interconnections, NOAA should provide an SLA to identify the level of service provided and connection expectations. Also, boundary level protection may be included in the SLA. For example, System ID NOAA0200 – the NOAA Network Operations Center – has defined an SLA for the subordinate system connecting to it in the Washington, D. C. area for Internet connectivity and shared security services. This SLA is sufficient for documenting the services offered by NOAA0200. Other areas of the country may utilize different NOAA systems for network/Internet connectivity and shared security services. A SLA should be in place where NOAA provides similar services to multiple systems. If no SLA exists, a MOU/A and ISA can be used. The SO should contact the NOAA point of contact to determine if a SLA exists or if interconnection documentation needs to be developed.

NESDIS also interconnects with other NOAA line offices for data exchange (e.g., National Weather Service). Since these systems typically require timely availability of data, an agreement should be created and maintained between NESDIS and the other NOAA line office. A MOU/A and ISA are required to document these types of interconnections. In situations where the data sharing is a one-to-many relationship, NOAA may choose to document this connection using a SLA instead of a MOU/A and ISA.

7.3.3 NESDIS-to-Government, Non-NOAA

NESDIS connections to other government agencies for network/Internet connectivity should be documented using a MOU/A and ISA. However, the other government agency may choose to document the connection using a SLA if they provide this service to a number of customers.

NESDIS maintains a number of interconnections with other government agencies for data sharing or shared security services. For these interconnections, a MOU/A and ISA are required. Interconnections for shared security services from one to many systems can be documented with a SLA instead of the MOU/A and ISA.

7.3.4 NESDIS-to-Academia/Scientific Community

NESDIS has a number of interconnections with external organizations in the academic and scientific communities. Dedicated or private connections to these organizations carry restrictive interconnection requirements that must be documented in an MOU/A and ISA. Technical details of the interconnection must be documented in an ISA. If the academic or scientific community is providing information to NESDIS, the interconnection must also detail the NESDIS data requirements in the MOU/A and ISA.

7.3.5 NESDIS-to-International

International interconnections should be documented in a MOU/A and ISA. International interconnections may require specific documentation requirements. Please contact the appropriate NESDIS International Affairs and NOAA General Council representative to ensure all requirements are met.

Some international agreements may not be able to have the requirements documented in a MOU/A and ISA as recommended by NIST SP 800-47. In these cases, the required topics described in NIST SP 800-47 should be appropriately addressed in the interconnection documentation, regardless of the document titles. As with all interconnection agreements, it is the AO who ultimately accepts the risk associated with the interconnection. The documentation should ensure all aspects of the interconnection are fully documented.

Please see Appendix A for a Technical Security Language Matrix for International Agreements.

7.3.6 NESDIS-to-Commercial Communications Service Provider

NESDIS may require connectivity using commercial communications circuits, either private/dedicated or shared. For these circuits, NESDIS should have fully documented, as part of the vendor's contract (or supplemental SLA), the availability requirements. In some cases, the vendor will also provide some level of confidentiality with the circuit. This information should also be documented. Data integrity is usually not part of the services offered for communications circuits; however, if the vendor is expected to provide integrity, it should be documented.

7.3.7 NESDIS-to-Other

For interconnection types not discussed above, the SO should follow the guidance in NIST SP 800-47 and create a MOU/A and an ISA to document the interconnection requirements. Any deviation from NIST SP 800-47 must be coordinated with the ITSO and the AO.

7.4 Determining Documentation Requirements

NESDIS provides an ISA template that 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 procedures below provide the steps for how to use the Table 1 to assist in determining what documentation is required for an interconnection.

Step 1. Determine the type of interconnection:

- a. NESDIS-to-NESIDS
- b. NESDIS-to-NOAA
- c. NESDIS-to-Government (non-NOAA)
- d. NESDIS-to-Academia/Scientific Community
- e. NESDIS-to-International
- f. NESDIS-to-Commercial Communications Service Provider
- g. NESDIS-to-Other

Step 2. Determine the Interconnection Purpose

- a. Network/Internet Connectivity
- b. Data Sharing
- c. Shared Security Services (one-to-one)
- d. Shared Security Services (one-to-many)

Step 3. Determine interconnection documentation requirements by using the matrix in Table 1 and section 7.0 of this document as a guide. The documentation requirements should be presented to the AO for final acceptance.

Step 4. Update the SSP to document the interconnection. In addition, develop the appropriate documentation using NIST SP 800-47 guidance. All security requirements and technical specifications of the interconnection should be documented in the interconnection documentation.

Step 5. Obtain AO approval for the interconnection using the methodology defined in NIST SP 800-47 and SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*.

Table 1. Minimum Interconnection Documentation Requirements

Interconnection Type	Interconnection Purpose	Documentation Requirements			
		SSP	SLA	ISA	MOU/A
NESDIS-to-NESDIS	Network/Internet Connectivity	X			
	Data Sharing	X			
	Shared Security Services (One-to-One)	X		X	
	Shared Security Services (One-to-Many)	X	X		
NESDIS-to-NOAA	Network/Internet Connectivity*	X	X	X	X
	Data Sharing	X		X	X
	Shared Security Services (One-to-One)	X		X	X
	Shared Security Services (One-to-Many)	X	X		
NESDIS-to-Government	Network/Internet Connectivity*	X	X	X	X
	Data Sharing	X		X	X
	Shared Security Services (One-to-One)	X		X	X
	Shared Security Services (One-to-Many)	X	X		

NESDIS-to-Academia/Scientific Community	Network/Internet Connectivity	X		X	X
	Data Sharing	X		X	X
	Shared Security Services (One-to-One)	X		X	X
	Shared Security Services (One-to-Many)	X		X	X
NESDIS-to-International	Network/Internet Connectivity	X		X	X
	Data Sharing	X		X	X
	Shared Security Services (One-to-One)	X		X	X
	Shared Security Services (One-to-Many)	X		X	X
NESDIS-to-Commercial Communications Service Provider	Network/Internet Connectivity**	X	X		
	Data Sharing				
	Shared Security Services (One-to-One)				

	Shared Security Services (One-to-Many)				
NESDIS-to-Other	Network/Internet Connectivity	X		X	X
	Data Sharing	X		X	X
	Shared Security Services (One-to-One)	X		X	X
	Shared Security Services (One-to-Many)	X		X	X
		*	For NESDIS-to-NOAA and NESDIS-to-Government Network Connectivity, either an SLA or both an ISA and an MOU/A is required.		
		**	For NESDIS-to-Commercial Communications Service Provider, the SLA requirements may be included in a commercial contract instead of a separate SLA.		

Appendix A: Technical Security Language Matrix for International Agreements

Date: July 7, 2011

Agreement Connection	MOU (Memorandum of Understanding)*	IA (Implementing Arrangement)**	PIP (Project Implementation Plan)***
Operational end-to-end connection	1	2a	3a
Operational direct readout (NESDIS pulls data direct from partner satellite and uses partner software)	1	2d	3c
Receipt of data for research purposes (non-operational)	1	2b if Partner pulls data 2c if <i>1-way push</i> from NESDIS to Partner	3b

* A **MOU** (aka MOA, or Memoranda of Agreement) is an agreement between two or more parties at the Agency level. MOUs must have correct legal authority, which is Joint Project Authority for most international agreements. A MOU project must further the mission of DOC, must have substantial involvement of all Parties, and costs must be “equitably apportioned” with benefits accruing to all Parties. MOUs provide a broad scope of cooperative activities for potential areas of collaboration, and include provisions or Articles that allow parties to conclude separate IAs or PIPs for specific activities.

** An **IA** is established at the Agency or Line Office level, is governed by a MOU, and is created for specific projects. There are often several IAs under one MOU.

*** A **PIP** is even more specific than an IA and details steps to be taken to implement a project.

NB: These terms are somewhat malleable. Depending on the project or Agency, a MOU may be more or less specific. Within NESDIS, we try to follow the above guidelines. Also, it is not necessary to have both an IA and a PIP. Sometimes one or the other is used, but regardless there is always a MOU to place the IA or PIP within.

1. MOU: Text in the MOU should create high-level awareness that applicable security considerations need to be addressed in subsequent PIPs or IAs. Suggested text to add is:
"The type of data to be exchanged and the mode of exchange, including any information security requirements for protecting data integrity and availability, shall be addressed in supplemental Implementing Arrangements and Project Implementation Plans, as applicable."
2. IA: Wording should be included that is more specific than the MOU as to the expectations for protection of the integrity and availability of data. The intent of this text is to put each party on notice that because the other party relies on the integrity of the connection and/or data and must have it available when needed (as specified in the IA requirements), that they are responsible for ensuring that appropriate security measures are in place. The following text is suggested:

2a. If an interconnection is established for 2-way exchange of data or products, include the following text: "Both parties agree that the information security measures implemented in performance of this arrangement shall ensure the highest level of integrity and availability of data exchanged, and that each Party shall comply with the other Party's requirements and policies governing data access. The security measures shall be consistent with recommendations of applicable standards, including

- International Organization for Standardization and International Electrotechnical Commission (ISO/IEC) standard 27001, *Information Security Management Systems--Requirements*
- Federal Information Processing Standard 200, *Minimum Security Requirements for Federal Information and Information Systems*"

In addition, if a Project Management Team is designated, include an information security Subject Matter Expert to advise the team on information security matters.

2b. If NOAA/NESDIS is providing a service whereby the foreign partner will only pull data from a NOAA/NESDIS server to which they have authorized access, insert the following text: "Access to and distribution of NOAA/NESDIS data shall comply with the requirements of the *NESDIS Policy on Access and Distribution of Environmental Satellite Data and Products* (17 February 2011)."

2c. If NOAA/NESDIS is sending data/products to a foreign partner server as a 1-way push, and NOAA/NESDIS has only a responsibility to meet partner requirements for data availability, then no additional text is required. It is the responsibility of the Partner to specify their requirements for data integrity and the NOAA/NESDIS system owner is responsible to ensure adequate security is in place to protect the NOAA/NESDIS system by preventing unauthorized response transmissions from the partner.

2d. If NOAA/NESDIS is accepting partner software for internal use to interpret satellite data pulled directly from a partner satellite, then the risk is on NESDIS to ensure that the software contains no malicious code and that the integrity of ingested data is assured.

The agreement should specify the following: “It is the responsibility of the XXXX (partner) to meet a XXXX (insert timeliness or percentage for availability expectation, such as 99%) level of availability of the satellite for data ingest.”

3. PIP: The PIP must contain explicit reference to minimum expectations for security. Suggested text follows:

3a. For interconnections, include the following text: “In order to foster public confidence in the data shared and the products generated based on that data, both parties agree to maintain an information security management program that will provide assurance that adequate protections for data integrity and availability consistent with the intent and framework of the following standards issued by the International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) (online at <http://www.iso.org/iso>) or the National Institute of Standards and Technology (NIST) (online at <http://csrc.nist.gov/>):

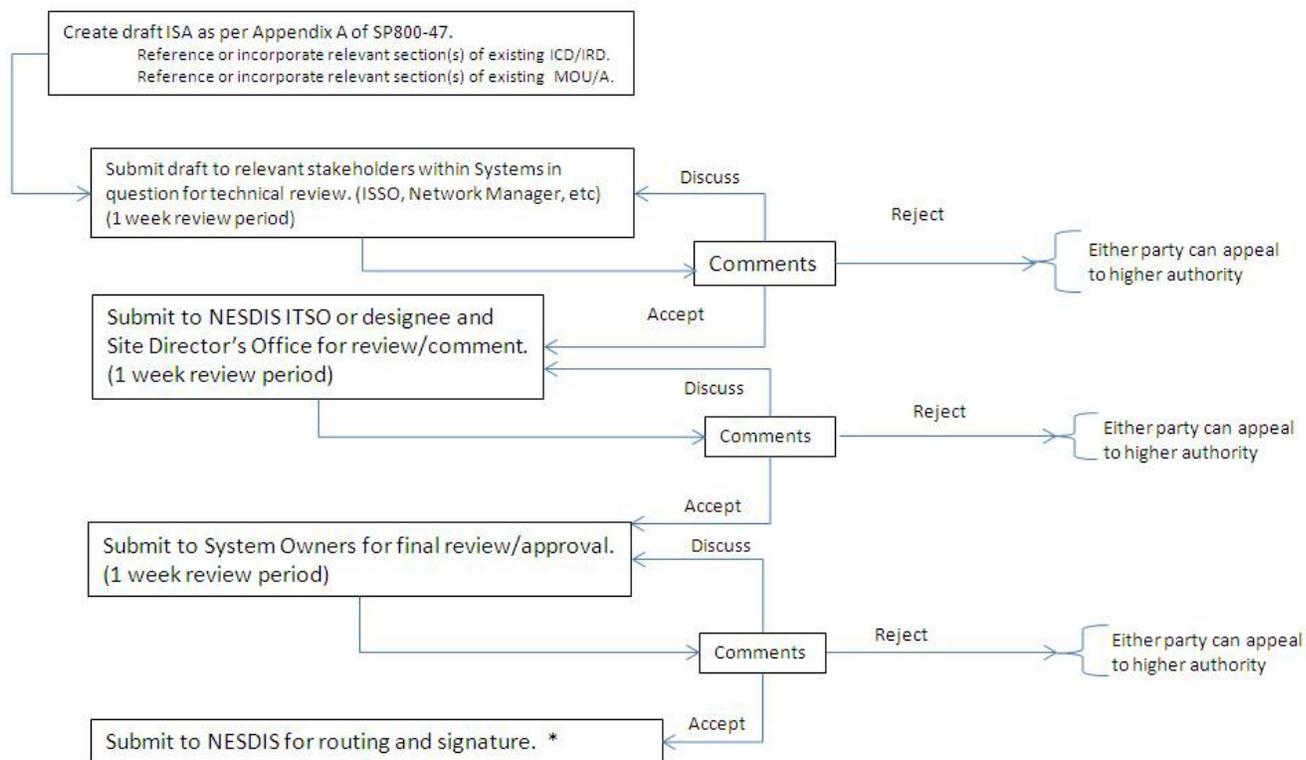
- ISO/IEC 18028-2 – *Information technology — Security techniques — IT network security — Part 2: Network security architecture*, February 2006
- ISO/IEC 27001 – *Information technology -- Security techniques -- Information Security Management Systems—Requirements*, October 2005
- ISO/IEC 27002 – *Information technology — Security techniques — Code of practice for information security management*, as amended July 2007
- NIST FIPS 200 -- *Minimum Security Requirements for Federal Information and Information Systems*, March 2006 (<http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf>)

“The Parties will ensure that the integrity of data is assured and accessible in a timely manner via an encrypted Internet connection (using technology approved at the Evaluation Assurance Level 4+ by the Common Criteria program, online at <http://www.commoncriteriaportal.org/> or equivalent) and with a service availability of no less than XX%. A supplemental Interconnection Security Agreement (ISA) or Service Level Agreement (SLA), as applicable, shall be executed in accordance with applicable U.S. and international standards for the adequate protection of information and information systems. In the execution of the ISA/SLA, all parties shall develop and implement programs for the adequate protection of information and information systems consistent with applicable U.S. and international standards as listed above.”

- 3b. “Access to and distribution of NOAA/NESDIS data shall comply with the requirements of the *NESDIS Policy on Access and Distribution of Environmental Satellite Data and Products* (17 February 2011).”
- 3c. “The XXX (Partner) shall maintain an adequate capability to meet the NOAA/NESDIS requirements for data availability. The XXX (Partner) shall employ

best practices in the development of software code used by NOAA/NESDIS for data analysis, and cooperate with NOAA/NESDIS as necessary in secure code reviews of software applications provided by the Partner.”

Appendix B: ISA Creation Workflow



*Need to identify appropriate secure document management environment – drafts or candidate versions of documents may not be appropriate for CSAM as delivery/distribution platform

System SO/ISSO will provide a formal disposition for all comments, with written responses. If a meeting/telecon is required to close any comment out, one will be coordinated.

Approval Page

Document Number: NQP-3411, Revision 2.1	
Document Title Block: Policy and Procedures for Determining Minimum Documentation Requirements for System Interconnections	
Process Owner: NESDIS Chief Information Division	Document Release Date: September 28, 2012

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
2.1	March 26, 2015	----	ALL	Baseline NQP-3411