NOAA/NESDIS

IT Systems Component Inventory Management Policy and Procedures

September 1, 2011

Prepared by:

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

Table of Contents

UNITED STATES DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric Administration
NATIONAL ENVIRONMENTAL SATELLITE. DATA
AND INFORMATION SERVICE
Siler 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 often 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 /111erconnections,* v2.1;
4. NESDIS *Contingency Planning Policy and Procedures,* v2. 1;
5. NESDIS *Policy and Procedures for Ensuring Security i11 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.l ;
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 011 NESDIS Information Systems,* v3.l.

These publications are part of the NESDIS-wide effort to maintain and enhance its foundation of NESDIS ITsecurity 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 Nancv.DeFrancesco@noaa.2ov or phone (30I) 713-1312.

NESDIS IT SYSTEMS COMPONENT INVENTORY MANAGEMENT POLICY AND PROCEDURES

Record of Changes/Revisions

Version	Date	Section	Author	Change Description
Draft 1.0	5/18/2010	All	Noblis	Initial Draft
Draft 1.1	6/20/2010	All	ITSO	ITSO edits
Final v1.2	9/1/2011	Headers, footers, Sections 1, 3.2, 3.3, 5, 6, 7.1.1, 7.1.2, 7.1.3, 7.2	ITSO	Address comments received on draft and finalize

1. Background and Purpose

Inventories have come to encompass a multitude of entity tracking functions and goals. The Department of Commerce (DOC) Information Technology Security Program Policy (ITSPP) refers to the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 control *CM-8 - Information System Component Inventory* which requires OUs to develop, document, and maintain a current inventory. The CM-8 control reflects the traditional understanding of an inventory as tracking physical assets and software for property management purposes. However, complete, thorough, detailed lists of all the system components (virtual and physical) that provide a potential communication path into the system are critical to the ability to fully assess risk to the system.

NESDIS recognizes four different inventories, one NESDIS program inventory and three system-specific:

- NESDIS Program Inventory
  - NESDIS Federal Information System Management Act (FISMA) inventory – a list of NESDIS systems (NOAA50xx)
- System-specific Inventories
  - Hardware inventory – a list of physical hardware
  - Software inventory – a list of all software packages and operating systems (commercial and freeware) installed on the components
  - Scan Inventory – a list of addressable instances, whether real or virtual.

The NESDIS FISMA inventory is maintained by the NESDIS Chief Information Division (CID). System Owners (SOs) are required to ensure that the FISMA inventory information maintained by the CID is current and accurate.

- The purpose of the hardware inventory is to track physical assets within the security boundary of the system. It shall support the identification of facility locations for hardware components that store information to permit appropriate disposal at the end of the component life. To support these purposes, NESDIS supplements DOC policy by extending the hardware inventory requirement to include non-networked components.

- The purpose of the software inventory is to manage the use of only authorized and properly licensed software and to track the revision, configuration, and installation status of that software for vulnerability facilitation.

- The purpose of the scan inventory is to track the addressable instances within the system to ensure complete and accurate vulnerability scanning. A full inventory of all addressable entities in the system is necessary to ensure that all entities scanned are authorized components of the system and that all instances are scanned by a vulnerability scanner.

2. Scope

This NESDIS Policy and Procedure (P&P) defines an inventory as a collection of assets (real or virtual) contained within or used within a NOAA50xx information system. The scope of this document is limited to addressing and augmenting requirements in ITSPP Section 4.5.6 (CM-8) for an inventory of physical and logical components that make up an information system and supporting ITSPP Section 4.15.6 (SA-6) *Software Usage Restrictions*.

3. Roles, Responsibilities, and Coordination

1. System Owners (SOs) shall coordinate with their Information System Security Officer (ISSO) and other support personnel as appropriate to ensure that the inventories appropriately reflect the composition of their system's hardware, software, and operating system instance implementation. The SO is responsible for ensuring that all software and hardware utilized on the system are appropriately licensed.
2. The Information System Security Officer (ISSO) shall support the SO to ensure that accurate, up-to-date inventories representing the actual state of the system are maintained, and that all hardware and software used is appropriately licensed—monitoring the management of inventories by other system personnel as appropriate and delegated by the SO.
3. System support personnel, as assigned by the SO, shall ensure that all entities and tracked configuration changes are reflected in the appropriate inventory in accordance with the system's configuration control process.

4. Management Commitment

The NESDIS CID supports the NESDIS Assistant Administrator's strong emphasis on securing NESDIS information and information systems. Through the issuance of this policy and accompanying procedures, it demonstrates their commitment for ensuring security and accountability in NESDIS inventory management practices.

5. Compliance

The NESDIS ITSO will review NESDIS inventories periodically for compliance with this policy and accompanying procedures. Compliance reviews will occur as part of the Assessment and Authorization process and as a part of the quarterly vulnerability scan analysis. The NESDIS ITSO may perform additional reviews at random intervals. Failure to maintain accurate, up-to-date inventories as described in this P&P may result in a conditional or denied Authorization to Operate (ATO), depending on the severity of the condition or systemic problems with inventory management. SOs found not in compliance with this policy will be reported to their Director and/or the system Authorizing Official (AO), as appropriate, and action may be taken, up to and including, removal from SO responsibilities.

6. Policy

NESDIS policy on the tracking of Information Technology (IT) assets is intended to enhance the applicability of the inventory as a basis for license management and IT security control assessments, including vulnerability scanning and penetration testing. NESDIS policy requires that SOs maintain three inventories documenting the contents of their system: a hardware inventory, a software inventory, and a scan inventory. Hardware, software, and scan inventories shall be maintained to reflect the current composition of the system as part of the system's continuous monitoring process.

6.1. Policy Maintenance

The NESDIS ITSO shall review this policy and procedures document biennially and update it 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.

6.2. Policy Feedback Process

NESDIS personnel are encouraged to notify the ITSO regarding any errors found in the document or other clarifications or updates that are required. Comments can be sent to the NESDIS IT Security Team by clicking on the bubble next to this document on the NESDIS IT Security Handbook web page at https://intranet.nesdis.noaa.gov/ocio/it_security/handbook/it_security_handbook.php and sending the comments to the provided address, or sending comments directly to nesdis.hq.secteam@noaa.gov.

6.3. Policy Effective Date

This policy is effective within 90 days of issuance.

7. Procedures

7.1. Inventories

Three types of inventories are to be maintained: the Hardware Inventory (see Appendix A template), the Software Inventory (see Appendix B template), and the Scan Inventory (see Appendix C template). Each of these is discussed in detail below.

7.1.1. Hardware Inventory

The hardware inventory shall list every IT hardware component associated with the system, including spares, new equipment awaiting deployment, and deactivated equipment that has not yet been excessed. Similarly, every hardware component shall be associated with a system. Every physical component that is assigned a tracking tag shall be listed in the hardware inventory. This includes subcomponents that are installed into other tracked hardware components.[1] NESDIS requires the hardware inventory to contain all hardware components, both networked and stand-alone computers. The hardware inventory shall be closely linked to the corporate asset management database, currently the Sunflower Asset Management System. Independent components such as Blackberries or other personal digital assistants (PDA) that send and receive e-mail or link with NOAA contact lists shall be associated with the administrative LAN that generally supports the user.

The DOC requires the hardware inventory be updated as an integral part of hardware component installations and as part of the Configuration Management process implementing CM-8 Information System Component Inventory. Transfer between systems of inventory controlled items shall be reflected as they occur in the respective systems. Inventory updates shall also occur in conjunction with the implementation of PE-16 Delivery and Removal

The hardware inventory record shall contain, at a minimum, the following items:

- Barcode/Property Number
- Hostname (the name used to identify the component on a network)
- Component Type: e.g. Server, router, workstation, switch, etc.
- Manufacturer
- Model
- Serial Number
- Component Revision Number: e.g. firmware version, etc.
- Physical Location: (include specific rack location for components in computer/server rooms)2
- Environment—the asset located either in a development, test, or production environment

[1] For example, an equipment chassis may contain numerous “blades” that were originally purchased together and listed under one barcode number for the entire chassis. However, if a blade in the chassis is replaced or an additional blade is added, the new blade is purchased separately and is assigned a new barcode number. There is now a rack of equipment with a barcode and a replacement blade that also has a barcode, but not all blades in the chassis have tags.

[2] For components that are installed into other tracked components (e.g. additional or replacement “blades” installed

within a chassis), the unique identifier for that component can be entered here. Mobile devices such as Blackberries should identify the person to whom they are assigned in this field.

The SO may add additional fields as necessary for local purposes.

7.1.2. Software Inventory

The Software inventory shall be used to track licenses and identify specific implementations of software products and packages. The specific implementation information includes version, revision numbers, and service pack, and is intended to support identification and mitigation when vulnerabilities are identified in software running on the system. The software inventory supports the implementation of SA-6 Software Usage Restrictions. Copyright and licensing information shall be maintained for all software products utilized on the system. Each software item shall be explicitly linked to each instance of the physical hardware that hosts the software, and if applicable, to each instance of a virtual machine on which the software runs. Users shall be prevented from unauthorized copying of Government licensed commercial software except through approved distributing that includes updating the software inventory.

Virtual machines are instances of operating systems running on a physical component where a physical component may host multiple instances of an operating system running at the same time. Typically, a virtual machine is an instance of an operating system that runs within another operating system. However, with advanced hardware, it is possible for the hardware to manage the operating system instances without a traditional host operating system. Each operating system has its own configuration and possible vulnerabilities. The ISSO must track and maintain every instance of each operating system. Likewise, software running within a virtual machine may be[3] considered a separate instance of the software for licensing purposes and therefore must be verifiable as appropriately licensed.

The SO shall maintain a complete list of software packages on each physical and logical entity in the inventories. Software inventory shall identify revision/service pack and the specific identification and configuration for every component upon which it is installed, including hardware components and virtual machines. The SO must track (at a minimum) the following software packages:

- All authorized user-controlled software installations
- All configuration controlled software (including each variant of the operating systems)
- Commercial and licensed products including licensed and used quantities
- Products that offer services to other components[4]

[3] Depending on manufacturer software licensing agreements. Software is typically licensed by installation, CPU, or site license. Regardless of the software license agreement, each installation must be tracked.

[4] Services include HTTP, FTP, RPC, etc. The service offerings do not have to cross the security boundary to meet this requirement.

- Major packages such as databases
- Office automation suites/products[5]
- Virtual Machine Hypervisors (Monitors)
- And software development environments.

The software inventory shall contain, at a minimum, the following items:

- Baseline Configuration (The unique identifier used internally for this specific baseline configuration that corresponds to the configuration item assigned in the Configuration Management Plan—some refer to this as a “build” or “image”)
- Software product name
- Version Number (includes revision number and service pack. May be split into a separate field)
- Configuration information
- License “(Commercial/Freeware/GNU Public License/Other - explain)
- License type (single user, multiple CPU, site license, perpetual or time limited)
- License Holder (point of contact or other information associated with tracking the license)
- License ID (if applicable. May be retained by site license administrator or other POC.)
- Method of License Enforcement (license server, keyed to CPU Serial number, online registration, local software installation, none, other)
- Host (the hardware or software entity hosting the instance)

Details of the license information may be kept with other personnel, such as parent organizations maintaining site or organizational licenses. The system software inventory must include the appropriate license information or details of where this information is maintained.

The SO may add additional fields as necessary for local purposes.

7.1.3. Scan Inventory

The scan inventory tracks network addressable entities and will be the basis for vulnerability scanning. The scan inventory includes the network interfaces for the devices listed in the Hardware Inventory, as well as virtual machines, dual-boot configurations, and multi-homed device interfaces. Every physical interface[6] shall be tracked in the scan inventory, as well as every virtual IP address and/or virtual machine. All addressable entities shall be identifiable by the physical hardware component hosting the entity and by the software which implements the entity.

[5] Microsoft Office, OpenOffice, etc.

[6] NIC Card, Network Port, Modem, etc.

The Baseline Configuration control CM-2 requires SOs to maintain configuration baselines that provide information about the components of an information system, including the standard software load for entities, such as operating system, installed applications with current version numbers, and patch information. Accurate configuration baselines permit sampling when performing control assessments, as documented in the NESDIS Control Assessment P&P. Every scan entity shall contain an entry identifying the baseline configuration implemented by the component, included in the list of scan inventory items below as "baseline configuration reference." The activation expectation of the operating system instance shall be provided to assist in determining the coverage of vulnerability scans. The activation expectation is an indication of the likelihood that an instance will appear in a scan and shall be expressed as a percentage of estimated uptime. This uptime reflects the anticipated usage of an instance and is not an indication of the reliability of the instance or the availability as expressed in a service level agreement. For example, a dedicated PC or a virtual machine that is intended to be operational at all times would have an activation expectation of 100%, while a dual-boot instance that is operational about half of the time would have an activation expectation of 50%. A virtual machine used only for testing by a developer may have an activation expectation of 5% or less.

Each operating system instance record shall include a comment field to provide specifics of the instance. Items to discuss in the comment field include a description how the instance is part of a cluster of hardware, cloud, etc. For complex environments such as cloud computing or virtual hosting, a document may be required to describe the environment.

The scan inventory shall contain, at a minimum, the following items:

- Hostname (the unique name which the entity uses to identify itself on a network)
- Entity Type (e.g. VMM, Virtual IP, physical NIC, etc.)
- IP Address
- MAC Address[7]
- Activation Expectation (percentage of estimated uptime)
- Baseline configuration reference
- Primary Administrator
- Host (the hardware or software entity hosting the instance)
- Comments

The SO may add additional fields as necessary for local purposes.

[7] MAC addresses do not need to be listed for every port on a switch.

7.2. Inventory Scenarios

The three inventories individually satisfy different control requirements (such as SA-6 and CM-8), but can be aggregated to create a full perspective of the system environment. A hardware device may host one or more scan entities. Each scan entity will likely, but not necessarily, have a corresponding software entry.[8]

Referring to Figure 1, *Virtual Server Implementation*, assume a system consists of an IBM server running AIX on which is running instances of separately addressable multiple Red Hat Linux virtual machines. The IBM server is documented in a HW inventory record, and the AIX and Linux licensing and configuration information are listed in SW inventory records. These entries are linked via the Host field in the SW Inventory record pointing to the Hostname field in the HW inventory record. In this instance, the Hostname and Host records will have identical values. The VM operating system instance and the Linux virtual machines are also documented in Scan inventory entries that also contain the Hostname and identifies the unique IP addresses and configuration details for each addressable entity. The virtual machine monitor overseeing the virtual machines operating on the server is a critical security-related item and has its own entry in the SW inventory.

Each separately addressable Red Hat operating system instance virtual machine is documented in a Scan Inventory entry that identifies the Hostname, addresses, and local configuration specifics. The Red Hat OS instance is also documented in a SW inventory record that includes the specifics of that Red Hat software installation and baseline configuration. Both the SW and Scan records are linked via the Hostname field. At the same time, the records are linked to the AIX instance via the Host fields of the Red Hat Scan and SW inventories pointing back to the Hostname of the AIX instance.

[8] A network appliance that is purchased and used as an unmodifiable device may not require a SW inventory entry.

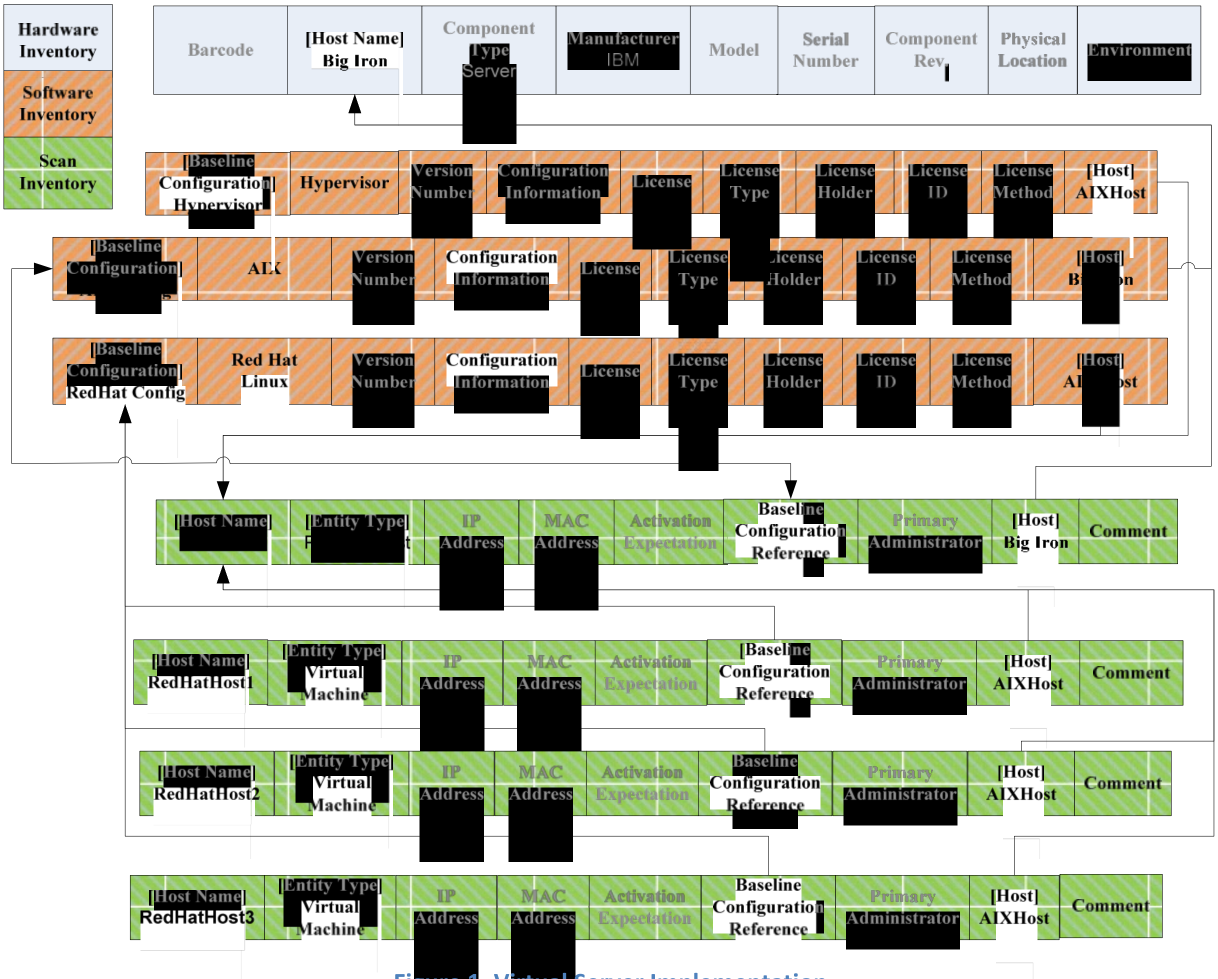

Figure 1. Virtual Server Implementation

Consider the scenario in Figure 2, *Virtual Player on Desktop*, in which a software developer uses a Red Hat Enterprise Desktop workstation to develop software and has a VMWare player to run a Windows environment for testing the software. The hardware is documented in a Hardware Inventory entry. There are Software Inventory records for the Red Hat Linux and Microsoft Windows operating systems, plus a Software Inventory record for the VMWare Player. The Red Hat Enterprise Desktop instance and Microsoft Windows instance are both represented by Scan Inventory records.

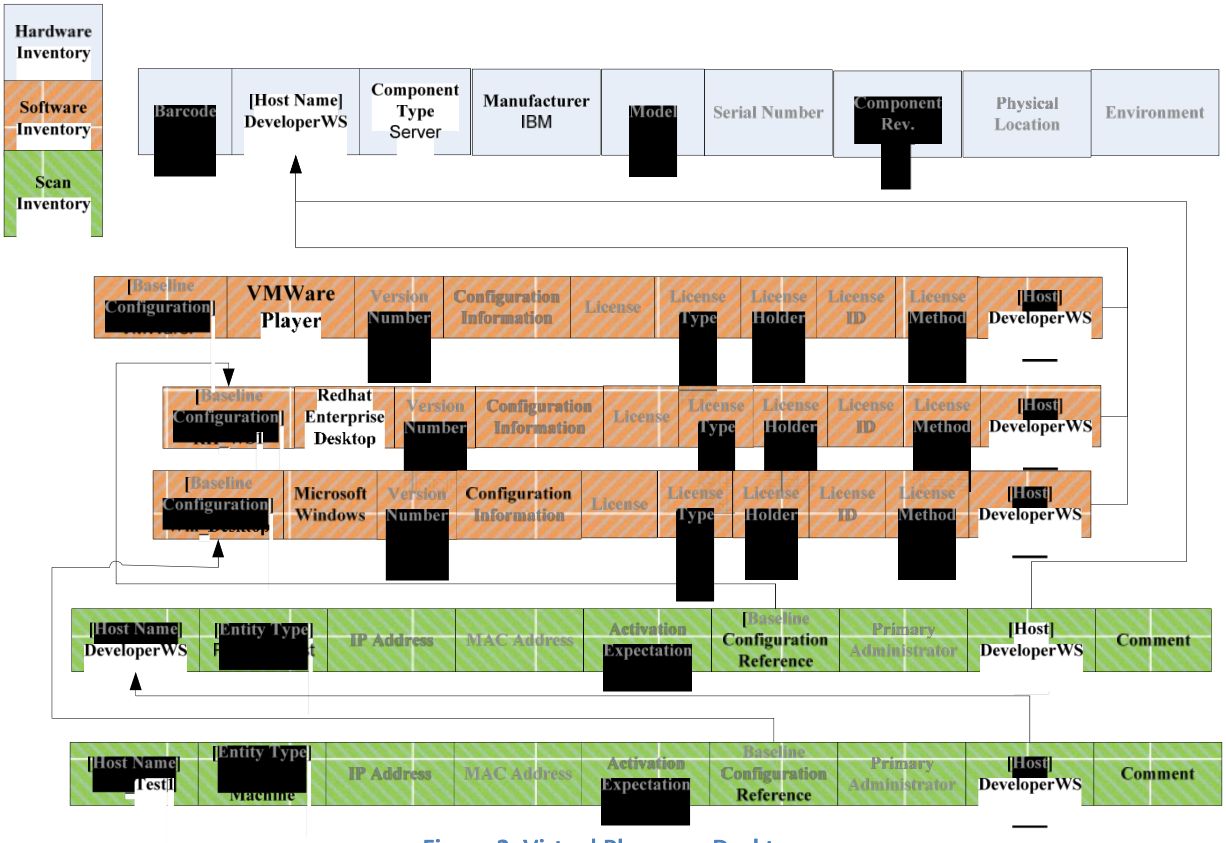

Figure 2. Virtual Player on Desktop

This page deliberately left blank

Appendix A: Hardware Inventory Template

Barcode	Hostname	Component Type	Manufacturer	Model	Serial Number	Component Rev.	Physical Location	Environment

Appendix B: Software Inventory Template

Baseline Configuration	Software Name	Version Number	Configuration Information	License	License Type	License Holder	License ID	License Method	Host

Appendix C: Scan Inventory Template

Hostname	Entity Type	IP Address	MAC Address	Activation Expectation	Baseline configuration reference	Primary Administrator	Host	Comment

Approval Page

Document Number: NQP-3416, Revision 1.3	
Document Title Block: **IT Systems Component Inventory Management Policy and Procedures**	
Process Owner: NESDIS Chief Information Division	Document Release Date: September 1, 2011

Prepared by:

Erica Boyd

3/26/15

Erica Boyd
Ambit- Associate Consultant
NESDIS Chief Information Office

Date:

Approved by:

Irene Parker

3/26/15

Irene Parker
Assistant Chief Information Officer - Satellites

Date:

Document Change Record

VERSION	DATE	CCR #	SECTIONS AFFECTED	DESCRIPTION
1.3	**March 26, 2015**	**----**	**ALL**	**Baseline NQP-3416**