

EPA Classification No.: CIO 2122-S-02.1	CIO Approval Date: 11/08/2013
CIO Transmittal No.: 13-007	Review Date: 11/08/2014

*Issued by the EPA Chief Information Officer,
Pursuant to Delegation 1-19, dated 07/07/2005*

Interim Update to the Personal Computer Configuration and Management Standard

1. PURPOSE

The EPA Personal Computer (PC) Configuration and Management Standard provides the information necessary to ensure a standardized, secure and reliable computing environment for the Agency. The Standard includes information on installation, configuration, and management of PC (including both desktop and laptop computers) hardware and software assets. This information is provided to serve three purposes:

- Provide a framework for PC configuration, upgrade, and replacement within EPA's IT environment.
- Ensure compatibility with other internal EPA systems and ensure the ability to share and edit documents.

Achieve efficiencies in technical support and management of the EPA IT infrastructure through standardization.

2. SCOPE AND APPLICABILITY

N/A

3. AUDIENCE

N/A

4. BACKGROUND

N/A

5. AUTHORITY

N/A

6. STANDARD

Effective Immediately:

- All workgroup (networked, shared) printers must default to black and white printing. Users may switch to color printing where there is a business need. This will result in a lower printing cost.
-

EPA Classification No.: CIO 2122-S-02.1	CIO Approval Date: 11/08/2013
CIO Transmittal No.: 13-007	Review Date: 11/08/2014

7. RELATED DOCUMENTS

N/A

8. ROLES AND RESPONSIBILITIES

N/A

9. DEFINITIONS

N/A

10. WAIVERS

N/A

11. RELATED PROCEDURES, STANDARDS AND GUIDANCE


N/A

12. MATERIAL SUPERSEDED

N/A

13. ADDITIONAL INFORMATION

N/A



Renee P. Wynn
**Acting Assistant Administrator for Environmental
Information
and Chief Information Officer
U.S. Environmental Protection Agency**

PREFACE TO SELECTED INFORMATION DIRECTIVES

CIO Transmittal No.: 15-010	CIO Approval Date: 06/12/2015
-----------------------------	-------------------------------

*Issued by the EPA Chief Information Officer,
Pursuant to Delegation 1-19, dated 07/07/2005*

CHIEF INFORMATION OFFICER MEMORANDUM

SUBJECT: Chief Technology Officer (CTO) Responsibilities in Selected Information Directives

Re-assigned CTO responsibilities

Effective immediately, CTO responsibilities detailed in the selected information directives (i.e., Information Policies, Procedures, Standards, and Guidance) listed in Appendix A are re-assigned to the OEI Office of Technology, Operations, and Planning (OTOP) Director and the Senior Agency Information Security Officer (SAISO) as detailed. The re-assignment does not change any requirements in the selected information directives.

The OEI Information Directives Program Manager is directed to attach this memorandum and Appendix A as a Preface to each of the Information Directives listed. OEI will then update the Roles and Responsibilities section of each Information Directive in accordance with the normal review and update cycle.



Ann Dunkin
Chief Information Officer
U.S. Environmental Protection Agency

APPENDIX A

Information Directive	Prior CTO Responsibilities	Re-assignment
CIO 2104.1 Software Management and Piracy Policy	Provide procedures, standards, and guidance to senior level managers to: support the Agency's Software Management and Piracy Policy and manage enterprise software licenses.	OTOP Director
CIO 2104-P-01.0 Software Management and Piracy Procedure	Provide procedures, standards, and guidance to senior level managers to: support the Agency's Software Management and Piracy Policy, manage enterprise software licenses, and provide covered users within their office with training and awareness on the Software Management and Piracy Policy through the annual Cybersecurity Awareness Training.	OTOP Director
CIO 2121.1 System Life Cycle Management (SLCM) Policy	Establish and publish procedures, technical operational procedures and standards (TOPS), and guidance supporting the Agency's SLCM Policy. Review and approve waivers to the SLCM Procedure.	OTOP Director
CIO 2121-P-03.0 SLCM Procedure	Establish and publish procedures, TOPS, and guidance supporting the Agency's SLCM Policy. Review and approve waivers to the SLCM Procedure.	OTOP Director
CIO 2122.1 Enterprise Architecture (EA) Policy	Issue procedures, guidance, and technical standards associated with the EA with a specific focus on the technology architecture, chair the Quality Technology Subcommittee (QTS), and review technology and security considerations in the Enterprise Target Architecture and Enterprise Transition Plan.	OTOP Director
CIO 2122-P-01.1 EA Governance Procedures	Issue procedures, guidance, and technical standards associated with the EA, with a specific focus on the technology architecture, chair the QTS, and review technology and security considerations in the Enterprise Target Architecture and Enterprise Transition Plan.	OTOP Director
CIO 2122-P-03.0 Information Technology Infrastructure Standard Procedure	Recommend to the CIO a specific IT standard, product or specification to be added to the official Agency IT Standards Profile with consultation from the Quality Information Council (QIC) and the QTS, and develop and maintain the Agency's Technology Architecture.	OTOP Director
CIO 2122-S-02.0 Personal Computer Configuration and Management Standard	Review and approve requests for waivers in regard to this standard.	OTOP Director
CIO 2123.1 Configuration Management Policy	Provide procedures, standards, and guidance to senior level managers in support of the Agency's Configuration Management Policy; institute change management processes; and provide a change management database.	OTOP Director

Information Directive	Prior CTO Responsibilities	Re-assignment
CIO 2150-P-01.1 Information Security - Interim Access Control Procedures	Approve all methods of dial-up access, approve all wireless connections, establish, document, authorize, and monitor all methods of remote access to an information system; delegate to Regions and other entities, as appropriate; and address co-management responsibilities for the Agency Security Architecture.	OTOP Director
CIO 2150-P-08.1 Information Security - Interim Incident Response Procedures	Determine Operational Status Categories during Alerts and Risks (OSCAR) 5 level (page 7).	SAISO
	Be available when the Computer Security Incident Response Capability (CSIRC) must report and coordinate incidents (page 16). Be available to meet with the Director of Cyber Security Staff (CSS) when senior managers are informed of incidents, occurrences and their status (page 18).	OTOP Director
CIO 2150-P-14.1 Information Security - Interim Risk Assessment Procedures	Approve the use of and, as appropriate, acquire and deploy enterprise vulnerability management technology. Consult with the SAISO to determine the coverage and compliance of enterprise vulnerability management technology with respect to federal and Agency requirements, including use of these tools to meet assessment requirements of other control families in NIST 800-53A, Revision 1, and to ensure the most cost effective, complete and accurate results.	OTOP Director
CIO 2150-P-15.1 Information Security - Interim System Services Acquisition Procedures	For the procurement of external information system services where a sufficient level of trust cannot be established, be available to confer regarding risks associated with the network and the Agency.	OTOP Director
CIO 2150-P-16.1 Information Security - Interim System and Communications Protection Procedures	Approve use of mobile VoIP-enabled units.	OTOP Director
CIO 2150.4 Mobile Computing Policy	Oversee policy and procedure implementation regarding use of mobile computing technologies. Approve mobile computing technology and device deployment.	OTOP Director
CIO 2150-P-01.1 Mobile Computing Management Procedures	Oversee policy and the implementation of the procedures. Approve enterprise mobile device types to be deployed. Review and approve requests for waivers in regards to the procedures.	OTOP Director

EPA Classification No.: CIO 2122-S-02.0	CIO Approval Date: 10/1/10
CIO Transmittal No.: 11-001	Review Date: 10/13

*Issued by the EPA Chief Information Officer,
Pursuant to Delegation 1-19, dated 07/07/2005*

Personal Computer Configuration and Management Standard

1. PURPOSE

The EPA Personal Computer (PC) Configuration and Management Standard provides the information necessary to ensure a standardized, secure and reliable computing environment for the Agency. The Standard includes information on installation, configuration, and management of PC (including both desktop and laptop computers) hardware and software assets. This information is provided to serve three purposes:

- Provide a framework for PC configuration, upgrade, and replacement within EPA's IT environment.
- Ensure compatibility with other internal EPA systems and ensure the ability to share and edit documents.
- Achieve efficiencies in technical support and management of the EPA IT infrastructure through standardization.

2. SCOPE AND APPLICABILITY

This Standard contains information on EPA Minimum PC System Configuration, PC Refresh Cycle, Green IT Operations, Asset Management, and Naming Conventions. The information contained in this document applies to all EPA- or contractor-owned or leased personal computers and software. EPA employee-owned and contractor-owned PCs used to perform government services at offsite locations are not covered under this Standard. PCs used for speciality or scientific purposes that are disconnected from the LAN do not fall under the scope of this Standard. However, these PCs still require appropriate protection and application of sound risk management principles, and must comply with the [OMB Memorandum M-08-22, Guidance on the Federal Desktop Core Configuration \(FDCC\)](#) security configuration where feasible and appropriate.

While this Standard covers aforementioned topics for Agency PCs, the PC Security Guidance, currently in draft, contains information and standard configurations related to antivirus and patch

EPA Classification No.: CIO 2122-S-02.0	CIO Approval Date: 10/1/10
CIO Transmittal No.: 11-001	Review Date: 10/13

management, network connections, encryption of mobile devices and computers, and other similar material.

3. AUDIENCE

The primary audience for the Personal Computer Configuration and Management Standard includes Local Area Network (LAN) and Desktop Administrators and other EPA personnel in roles that are directly responsible for the configuration, management, oversight, and successful day-to-day operations of EPA personal computers.

4. BACKGROUND

EPA personnel share common missions, yet each organizational unit has unique requirements and expectations for system reliability and performance. Each LAN and Desktop Administrator must be able to provide required services for their customer without sacrificing the integrity of the network. Application developers and service providers must deliver systems that work at any EPA site. The diversity of personal computer hardware and software makes this an arduous undertaking, and applying a common hardware and software standard and configuration is a key goal meant to minimize potential system configuration conflicts.

EPA's network infrastructure and technology continues to evolve rapidly in response to program mission needs, regulatory drivers and enterprise architecture refinements. Originally, the Agency's IT infrastructure network was decentralized, necessitating that LAN and PC configuration be managed locally with integration only possible within the immediate facility network. Today EPA's IT network links all local LANs into a national backbone network consisting of more than twenty-six thousand personal computers and file servers. The complexity of the network requires a management approach that relies on the skills and talents of many IT professionals at the local level in addition to oversight by the Agency's IT management organizations with requisite authority to align the network with EPA's enterprise architecture and ensure security and continuity of operations. Thus, the importance of clearly defined and followed standards for equipment, software, and operating procedures is vital to providing reliable and secure services.

This standard fulfills the [Federal Desktop Core Configuration \(FDCC\)](#) mandate, issued by the Office of Management and Budget (OMB), Memorandum M 07-11 on March 22, 2007, which requires federal agencies to standardize desktop configurations to meet FDCC standards. This Standard also fulfills [Executive Order 13423](#), which requires that all agencies improve stewardship during procurement, use and disposal of federal electronics. E.O. 13423 sets specific targets for procuring energy efficient electronics, managing power, and recycling retired equipment in order to reduce negative impacts on the environment.

EPA Classification No.: CIO 2122-S-02.0	CIO Approval Date: 10/1/10
CIO Transmittal No.: 11-001	Review Date: 10/13

5. AUTHORITY

This Standard is issued under the authority of:

- The [Agency Network Security Policy](#), EPA Classification No. 2150.0. Specifically, Section 6.3.2 of the Agency Network Security Policy provides that all network-attached resources must conform to a standard configuration established by the Agency.
- The [Software Management and Piracy Policy](#), EPA Classification No. 2104.0. This policy requires that all software installed on EPA computer systems, including personal computers and servers, is appropriately licensed and approved for use, and is not pirated software.
- The [Enterprise Architecture Policy](#), EPA Classification No. 2122 establishes the EPA Enterprise Architecture Program. The Enterprise Architecture Policy establishes how IT investments are evaluated for compliance with the Enterprise Architecture and aligned with EPA's mission, goals, and objectives.
- [Executive Order \(E.O.\) 13423, Strengthening Federal Environmental, Energy, and Transportation Management](#), signed by President George W. Bush on January 24, 2007, requires that all agencies improve stewardship during procurement, use and disposal of federal electronics.
- Information Security Configuration Management Procedures, still in draft.
http://epaquickplace1.rtp.epa.gov/QuickPlace/technologyandinformationsecurityforum/Pages/Library852575700053B0C8.nsf/h_Index/FC8E4A87499FF77385257571007001A0/?OpenDocument
- The Office of Management and Budget (OMB) Memorandum M-07-11, [Implementation of Commonly Accepted Security Configurations for Windows Operating Systems](#), published March 22, 2007. This Memorandum is an OMB issued policy requiring agencies using or acquiring Windows XP and VISTA to adopt the Federal Desktop Core Configuration by February 1, 2008. This policy is consistent with 44 U.S.C. § 3544(b)(2)(D)(iii) of the Federal Information Security Management Act (FISMA) of 2002, which requires agencies to ensure compliance with minimally acceptable security configurations when acquiring information technology.
- The Office of Management and Budget (OMB) Memorandum M-07-18, [Ensuring New Acquisitions Include Common Security Configurations](#), published June 1, 2007. This directive provides language for all federal agencies to use in solicitations to ensure new acquisitions include FDCC security configurations and for information technology providers to certify that their products operate effectively using these configurations.
- The Office of Management and Budget (OMB) Memorandum M-08-22, [Guidance on the Federal Desktop Core Configuration \(FDCC\)](#), published August 11, 2008. This OMB memorandum requires that all federal agency information technology providers use Security Content Automation Protocol (SCAP) validated tools to certify that their products operate correctly with FDCC configurations and do not alter FDCC settings. It further states that agencies must use SCAP tools to scan for both FDCC configurations and configuration deviations approved by department or agency accrediting authorities. Agencies must also use these tools when monitoring use of these configurations as part of FISMA continuous monitoring.

EPA Classification No.: CIO 2122-S-02.0	CIO Approval Date: 10/1/10
CIO Transmittal No.: 11-001	Review Date: 10/13

6. RELATED DOCUMENTS

The following documents cover topics related to this Standard:

- EPA Personal Property Policy and Procedure Manual. The Manual presents policy and procedural guidance on personal property management issues for EPA employees and contractors. <http://intranet.epa.gov/oaintran/fmsd/property/pdfs/pp-policy-procedures-manual.pdf>
- LAN Operating Procedures and Standards (LOPS) <http://intranet.epa.gov/nis/lops.html>. The LOPS manual provides a reference for LAN implementation and operation within the EPA's standardized framework.
- Personal Computer Security Guidance (currently in draft). This Guidance contains information and standard configurations related to antivirus and patch management, network connections, encryption of mobile devices and computers, and other similar material.
- Policy on Limited Personal Use of Government Office Equipment, EPA Document # CIO 2101.0 (formerly 2100.3 A1) <http://intranet.epa.gov/ohr/rmpolicy/ads/orders/2100.3A1.pdf>. This policy prohibits employees from loading personal software onto EPA PCs or making any related configuration changes, unless approved by an appropriate information technology manager.

7. STANDARD

Minimum PC System Configuration

This Standard establishes the authority to set, and revise, EPA's minimum PC configuration standard. The IT Standards Profile site is the authoritative site for the current minimum PC configuration standard. Offices may exceed the minimum standard if they deem it the best value for the Agency. Please refer to the [EPA IT Standards Profile](http://intranet.epa.gov/itstandards) site (<http://intranet.epa.gov/itstandards>) for the most current information on minimum PC configurations.

EPA's minimum PC configuration standard is reviewed annually to ensure responsiveness to the changing IT environment. Any proposed changes go through the QTS to the CTO for a final recommendation for approval to the CIO.

This minimum configuration standard ensures that all future PCs have adequate hardware to support emerging technology needs for a minimum of four years, which corresponds to the Agency's PC refresh cycle. EPA's minimum PC configuration standard also meets the requirements of the [Federal Desktop Core Configuration \(FDCC\)](#) mandate under OMB Memorandum M 07-11.

EPA Classification No.: CIO 2122-S-02.0	CIO Approval Date: 10/1/10
CIO Transmittal No.: 11-001	Review Date: 10/13

PC Refresh Cycle

Electronics are the fastest growing portion of the municipal waste stream. The Federal Government disposes of approximately 10,000 computers every week. The President issued an Executive Order ([Executive Order 13423](#)) to all Federal Agencies in 2007 to take steps to limit the impact on the environment of the electronics that are used. One step in doing so is to set minimal standards for refresh of electronics, including standard PCs. Establishing an appropriate refresh cycle must be balanced between the requirements to fulfill the Agency's mission and the need to minimize the environmental impact of electronics, including PC disposal, and consistent with the mission of the Agency to protect the environment. To comply with E.O. 13423, EPA has established a four-year life-cycle for Agency PCs, which is an industry best practice. In addition to protecting the environment, this mandatory PC life-cycle helps to ensure that all Agency employees have access to current technology.

All existing EPA PCs must be upgraded or replaced to meet the minimum standard according to the adoption date published on the [EPA IT Standards Profile](#) site (<http://intranet.epa.gov/itstandards>). A PC that does not meet this minimum configuration and is not current in a 4 year refresh cycle, but is necessary to support an approved software application, must be disconnected from the Agency network by the published adoption date. PCs at EPA will follow a standard refresh lifecycle that encompasses the acquisition, deployment, maintenance and retirement phases. Each of these lifecycle stages has its own unique considerations.

Acquisition

- Confirm that new PCs meet the EPA minimum PC hardware configuration (refer to <http://intranet.epa.gov/itstandards>).
- Select a configuration that can reasonably be anticipated to meet needs for four (4) years and that is both ENERGY STAR® certified and an Electronic Product Environmental Assessment Tool (EPEAT, <http://www.epeat.net>) registered product. ENERGY STAR® refers to the certification of energy efficiency of equipment to help reduce greenhouse gases. When selecting the configuration, efforts should be made to procure EPEAT Silver rated electronic products or higher if available.

Deployment

- Upon delivery of leased or purchased equipment, all PCs should receive a property tag and be entered into an asset management database.
- Ensure that new PCs are configured per EPA minimum requirements as outlined in the appropriate Standard Configuration Document found at <http://intranet.epa.gov/itstandards>.
- ENERGY STAR® settings must be enabled on the PC.

Maintenance

- Identify the maintenance support mechanism (e.g., contract with service provider, service-level agreement (SLA), or call center) to keep PC configuration current.
- Produce an Assessment Report (AR), which displays inventory status on an annual

EPA Classification No.: CIO 2122-S-02.0	CIO Approval Date: 10/1/10
CIO Transmittal No.: 11-001	Review Date: 10/13

basis for management of the replacement/upgrade process.

Retirement

- Identify candidate PCs for retirement at each annual assessment.
- Sanitize all necessary components on replaced PCs in accordance with the [EPA Disk Sanitization Procedure](#).
- All retired electronic products are re-used, donated, sold or recycled using environmentally sound management practices and in compliance with EPA's Personal Property Policy and Procedure Manual (<http://intranet.epa.gov/oaintran/fmsd/property/pdfs/pp-policy-procedures-manual.pdf>).

The following diagram represents possible checkpoints and relative timeframes for managing the typical PC refresh cycle. It is not intended to limit procurement to the end of the fiscal year but instead represents a full four-year timeframe that coincides with government fiscal years as an illustrative example for the cycle.

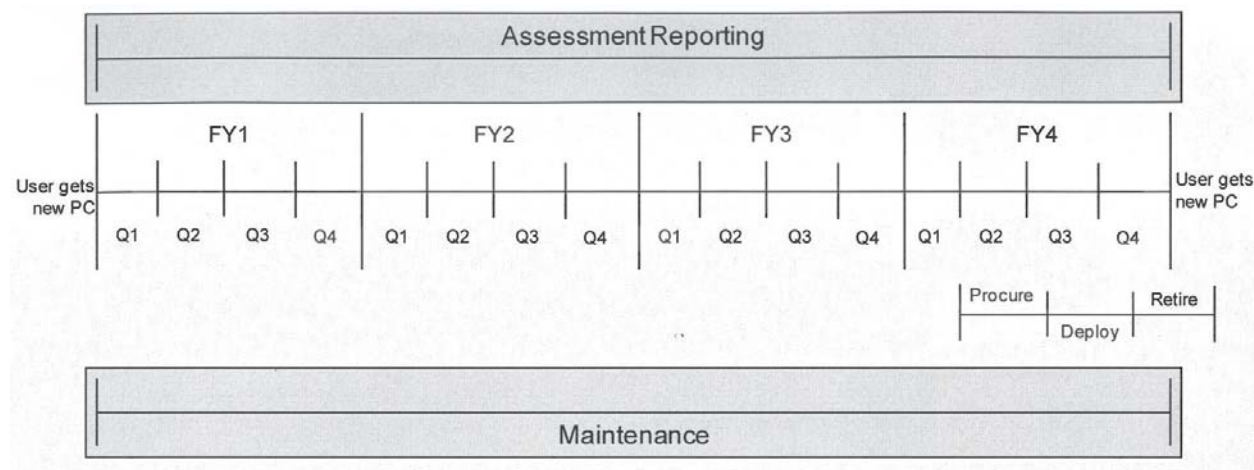


Figure 1: Refresh Cycle

As shown in the figure above, the process for replacing a PC at the end of its 4-year life cycle begins at the start of Q2 of the PC's fourth year. At this point, the process steps outlined above begin. Maintenance activities occur throughout the life cycle of the PC.

Green IT Operations

Executive Order 13423 sets goals for Federal Agencies in the areas of energy efficiency, acquisition, renewable energy, toxics reductions, recycling, sustainable buildings, electronics stewardship, fleets, and water conservation. In the area of electronic stewardship, the Executive Order listed specific requirements for operations of electronics.

Specifically:

- ENERGY STAR® compliant computers and monitors should be purchased whenever feasible. A computer certified as ENERGY STAR® compliant can save the Agency \$25 to \$75 per desktop computer annually.
- Each monitor must be set to enter sleep mode after 10 minutes of inactivity.

EPA Classification No.: CIO 2122-S-02.0	CIO Approval Date: 10/1/10
CIO Transmittal No.: 11-001	Review Date: 10/13

- Each computer must be set to turn off hard disks after 60 minutes of inactivity and enter standby mode after 60 minutes of inactivity.
- Employees must power down (turn off) both the computer and the monitor at the end of each day, unless otherwise instructed. This will result in significant energy savings for the Agency.
- All workgroup (networked, shared) printers must be set to default to duplex printing and enable sleep mode (if available) after 60 minutes of inactivity. Users may have the ability to print single-sided.
- All toner cartridges, and other packing materials and supplies, must be recycled to the greatest extent possible.
- All electronics purchased should be rated EPEAT Silver, or higher, if available.

Additional information on Green IT Operations can be found at www.energystar.gov, and EPEAT at <http://www.epeat.net>.

Asset Management

Each program office is responsible for creating and maintaining an inventory of their IT hardware and software. At a minimum, the inventory must include acquisition dates, property descriptions, associated licensing information, and serial numbers for all items. The inventory must track both software and hardware procurements. Program offices must be able to provide an inventory of IT equipment if requested.

More information regarding asset management can be found in EPA's Personal Property Policy and Procedure Manual (<http://intranet.epa.gov/oaintran/fmsd/property/pdfs/pp-policy-procedures-manual.pdf>).

Personal Computer Naming Conventions

At EPA, use of a standardized naming convention is imperative for uniquely identifying and managing EPA's computers. EPA's naming convention serves several important purposes, including:

- Takes the guesswork out of naming new IT equipment and helps to reduce naming conflicts between systems;
- Conveys important information about the specific pieces of equipment and allows EPA to easily locate network resources, improve search effectiveness, and simplify network administration and troubleshooting;
- Identifies the owner of the system that may have a security vulnerability, so that remediation can be applied in a timely manner to limit the risk to EPA's network; and
- Adds a level of security to EPA's IT assets by making it more difficult for hackers and unauthorized persons to identify system resources.

EPA's naming convention works to ensure IT system viability and security through the use of standard, consistent, and meaningful names. These are:

- All computer names must be unique within the network, and have a maximum length of 15 characters (with no spaces). Characters should be alphanumeric, with no dashes (-) or underscores (_).
- Two separate computer types are designated: D = Desktop and L = Laptop.
- If the computer is managed by CTS, the letter C is added to the computer type.

EPA Classification No.: CIO 2122-S-02.0	CIO Approval Date: 10/1/10
CIO Transmittal No.: 11-001	Review Date: 10/13

- The RPIO AHRC Code is a set of codes used to designate the responsible program office. (The RPIO AHRC Codes can be found in the next section.)
- The Secure Identity Management (SIM) user ID is an employee's unique LAN log-in name or ID. If multiple users have the same first initial and last name, or if a user has multiple assigned computers, a numerical identifier is used (e.g., JJones02). The SIM-EPA user ID and the numerical identifier combined may not exceed 8 characters.
- EPA Computers that are used for public use and for training purposes, and are not currently assigned to SIM, must be assigned and should be given useful identifiers, such as Train (computers used for training purposes), and Pub (computers available to the public).

Example:	Computer Type	RPIO AHRC Code	SIM-EPA User ID
	DC	1818T	KSmith02

Resulting PC Name: DC1818TKSmith02. This PC name indicates a CTS-managed desktop computer owned by the Office of Environmental Information (OEI) assigned to user K. Smith. The naming convention limits PC names to 15 characters. Do not exceed the 15 character limit.

RPIO AHRC Codes

The RPIO and AHRC codes together are five character accounting codes. Each location should be aware of their applicable codes for inclusion in the personal computer names. The Responsible Program Implementation Office (RPIO) code is a 2-digit numeric code that provides a unique identifier for each EPA Program Office and Region. RPIO codes are listed in the table below.

Table 3: RPIO Codes

Office	RPIO Code
Region 1 – Boston, MA	01
Region 2 – New York, NY	02
Region 3 – Philadelphia, PA	03
Region 4 – Atlanta, GA	04
Region 5 – Chicago, IL	05
Region 6 – Dallas, TX	06
Region 7 – Kansas City, KS	07
Region 8 – Denver, CO	08
Region 9 – San Francisco, CA	09
Region 10 – Seattle, WA	10
Office of the Administrator (AO)	11
Office of Internal Affairs (OIA)	13
Office of Administration and Resource Management (OARM)	16
Office of the Chief Financial Officer (OCFO)	17

EPA Classification No.: CIO 2122-S-02.0	CIO Approval Date: 10/1/10
CIO Transmittal No.: 11-001	Review Date: 10/13

Office of Environmental Information (OEI)	18
Office of Prevention, Pesticides, and Toxic Substances (OPPTS)	20
Office of Research and Development (ORD)	26
Office of Air and Radiation (OAR)	27
Office of Water (OW)	30
Office of Inspector General (OIG)	35
Office of General Counsel (OGC)	39
Office of Solid Waste and Emergency Response (OSWER)	75
Office of Enforcement and Compliance Assurance (OECA)	77

Allowance Holder (AH) codes are 2-digit numeric accounting codes that vary by Office. Responsibility Center (RC) codes are at least 1 alphanumeric character and also vary by office. AHRC codes are available by contacting your RPIO Coordinator, Senior Budget Officer (SBO) or your WCF Service Agreement Originator. A list of RPIO Coordinators is maintained at the following web site: <http://intranet.epa.gov/ocfo/wcf/rpiocoordinators.htm>

8. ROLES AND RESPONSIBILITIES

All users of EPA personal computers and/or software, including EPA contractors, are responsible for adhering to this standard.

Chief Information Officer (CIO) is responsible for ensuring implementation of this standard throughout the Agency.

Chief Technology Officer (CTO) is responsible for reviewing and approving requests for waivers in regards to this standard.

Senior Information Officials (SIO) are responsible for implementing this standard within their organization.

Information Management Officers (IMOs) & Information Resource Management Branch Chiefs (IRM BC) are the approving authority for purchase and use of software within their office (excluding enterprise software) and are responsible for carrying out procedures that support compliance with the standard within their office. IMOs are also responsible for addressing questions and concerns related to any implementation issues inherent in this standard.

Information Security Officers (ISO) are responsible for ensuring that responsible program offices and individuals throughout their Program or Regional Office are cognizant of security requirements and processes, and addressing questions and concerns related to any security-related issues inherent in this standard.

Program offices are responsible for creating and maintaining an inventory of their IT equipment. The inventory must track both software and hardware procurements and include acquisition dates, property descriptions, associated licensing information, and serial numbers for

EPA Classification No.: CIO 2122-S-02.0	CIO Approval Date: 10/1/10
CIO Transmittal No.: 11-001	Review Date: 10/13

all items.

Managers are responsible for addressing incidents of non-compliance with this standard. Managers are also responsible for answering questions from employees regarding this standard.

Quality Technology Subcommittee (QTS) considers proposals to set new standards, and forwards recommendations thru the CTO to the CIO for approval.

The Office of Environmental Information, Office of Technology Operations and Planning, Enterprise Desktop Solutions Division (OEI-OTOP-EDSD) is responsible for addressing questions and concerns regarding interpretation of this standard.

9. DEFINITIONS

AHRC Code – Office Account Holder Responsibility Center is a code that can be alpha-numeric which is used to provide a unique identifier for each organization within EPA. AHRC codes are available by contacting your RPIO Coordinator, Senior Budget Officer (SBO) or your WCF Service Agreement Originator. A list of RPIO Coordinators is available at:
<http://intranet.epa.gov/ocfo/wcf/rpiocoordinators.htm>

EPA Network – a system containing any combination of EPA computers, computer terminals, printers, audio or visual display devices, or telephones interconnected by telecommunication equipment or cables

EPA Production Environment – any computing resource (including servers, printers, and PCs) that is physically connected to the EPA network

EPA UserID – an EPA employee's unique LAN log-in name and/or identification

Enterprise Architecture – a strategic information asset base that provides a definition of the mission, the information and technologies necessary to perform the mission, and transitional processes for implementing new technologies in response to changing mission needs (CIO 2122)

Information - any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual forms

Information Technology - any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by an executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which (i) requires the use of such equipment, or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term "information technology" includes computers, ancillary

EPA Classification No.: CIO 2122-S-02.0	CIO Approval Date: 10/1/10
CIO Transmittal No.: 11-001	Review Date: 10/13

equipment, software, firmware and similar procedures, services (including support services), and related resources. The term "information technology" does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract. The term "information technology" does not include national security systems as defined in the Clinger-Cohen Act of 1996 (40 U.S.C. 1452)

Patch - Also called a service patch, a fix to a bug add additional functionality, or repair a security vulnerability. Patches are typically applied to operating systems, but can also be applied to applications if necessary. A patch is an actual piece of code that is inserted into (patched into) an executable program

PC – The term 'PC' includes all Agency owned laptop and desktop computers. In the case of desktop computers, the term 'PC' includes both the CPU and monitor

Personal Property – Any property, except real property, including EPA PCs and associated software.

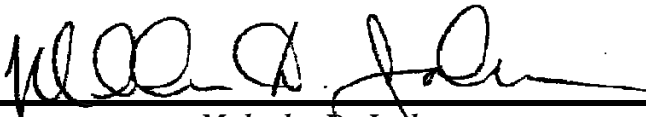
RPIO – the Responsible Program Implementation Office code is a static number that is generally used for account purposes to provide a unique identifier for each organization within EPA. RPIO codes are listed in Section 7.1.2.

SIM – the Secure Identity Management (SIM) user ID is an employee's unique LAN log-in name or ID

Virus – A program or piece of code that is loaded onto a personal computer without the user's knowledge. Viruses are dangerous because they can quickly use all available memory and bring the system to a halt. An even more dangerous type of virus is one capable of transmitting itself across networks and bypassing security systems

13. ADDITIONAL INFORMATION

For questions about this Procedure, please contact the Office of Environmental Information, Office of Technology Operations and Planning, Mission Investment Solutions Division at (202) 566-0330.



Malcolm D. Jackson
*Assistant Administrator for Environmental Information
 and Chief Information Officer
 U.S. Environmental Protection Agency*