

**United States Department of Commerce  
National Oceanic and Atmospheric Administration**



**NOAA FDCC Implementation Plan**

Version 1.0

## Record of Changes/Revisions

Modifications made to the plan are recorded in the Change/Revision Record below. This record shall be maintained throughout the life of the document.

Version No.	Date	DESCRIPTION OF CHANGE	Pages Affected/Section	Change Made By
0.5	10/1/2007	Initial Draft	All	L. Reed
0.6	10/17/2007	Update to the GPO section to include conf. working groups options		L. Reed
0.7	11/26/2007	Updated schedule, standalone deployment and GPO		L. Reed
0.8	11/28/2007	Updated NOAA Secure config policy reference	Background	L. Reed
0.8	11/28/2007	Updated Remote Systems Strategy section to utilize tools created for standalone systems	Remote Systems	L. Reed
0.8	11/28/2007	Updated Appendix A to include complete membership list		L. Reed
0.8	11/28/2007	Added reference to NIST/Census coordination	Collaboration	L. Reed
0.9	11/28/2007	Update TOC, correct spelling errors/typos		L. Reed
1.0	12/4/2007	Update reporting dates		L. Reed

## Table of Contents

Background.....	4
Phased Implementation Plan.....	4
Phase I: Identify Scope and Establish Policy.....	4
Phase II: Identify and Test Applications.....	5
Phase III: Deployment.....	5
User Notification.....	5
Collaboration.....	5
Implementation.....	6
Active Directory Environments.....	6
Standalone Internal Systems.....	7
Remote Systems.....	10
Schedule.....	10
Reporting.....	12
Phase IV: Monitoring and Compliance.....	12
Waivers.....	12
Appendix A ITSC Working Group and Task Force Charters.....	14
NOAA IT Security Committee Working Group Terms of Reference.....	14
Working Group Name:.....	14
Purpose:.....	14
Roles and Responsibilities:.....	16
Decision Making Process:.....	16
Charter:.....	16
Authority:.....	16
Schedule and Deliverables:.....	16
Resources:.....	17
TASK FORCE – IMPLEMENTATION.....	18
TASK FORCE – CONFIGURATION.....	19
Appendix B NOAA All Hands Memorandum.....	21
Appendix D. VB Script for standalone systems.....	22

## Background

The Office of Management and Budget recently issued policy memorandum M-07-11, "Implementation of Commonly Accepted Security Configurations for Windows Operating Systems," which stated: "agencies with these operating systems [Windows XP and VISTA] and/or plans to upgrade to these operating systems must adopt these standard security configurations by February 1, 2008." Subsequently OMB and NIST have defined the Federal Desktop Core Configuration as the standard security configuration. NOAA has adopted policy, [NOAA Secure Configuration for Windows Policy \(NISN 4.001\)](#), that supports the OMB memo.

NOAA's mission has many facets that reach from the bottom of the ocean to high orbiting satellites. Because of the wide breath of these missions, desktop management is decentralized across all Line and Staff offices throughout the nation. To say the least, standardizing on a security configuration on a national level will present many challenges and will not be a trivial project. None the less, NOAA is committed to improve its security posture by reducing the variety and, therefore the complexity, of supporting multiple operating systems on desktops and laptops.

The NOAA IT Security Committee, working under the authority of the CIO Council, has established a working group to facilitate the testing, implementation, and reporting of the FDCC implementation.

The VISTA operating system is currently being tested and will be configured in accordance with the FDCC before deployment. Therefore this plan is focused on Windows XP.

### ***Phased Implementation Plan***

NOAA will use a phased approach to the project. While some tasks may have dependencies, there are other tasks that may be able to run in parallel with other tasks. This may be advantageous when considering the OMB deadline of February 1, 2008. The five phases of this project are as follows:

Phase I: Identify Scope and Establish Policy

Phase II: Identify and Test Applications

Phase III: Deployment

Phase IV: Monitoring and Compliance

### **Phase I: Identify Scope and Establish Policy**

The scope of the OMB M-07-11 requirements have been defined by OMB and

clarified by [NOAA IT Standard 4.001 Secure Configuration for Windows Operating System](#). This plan is focused on Microsoft Windows XP Operating systems. NOAA Line Offices must determine the quantity of Windows XP systems and establish a mechanism to maintain this information. In lieu of an enterprise asset management tool each LO should plan to manage this information. It is critically important to ensure all devices within scope are tracked. Processes and procedures should be developed to maintain compliance with this policy as it relates to new systems, existing systems, and systems that are decommissioned. Devices include local systems, remote systems, and laptops.

## **Phase II: Identify and Test Applications**

The NOAA IT Security Committee working group has created a task force to perform application testing. The task force began on October 10, 2007. Appendix A includes the task force charter. The task force created a testing methodology document and results form to be used by everyone that is performing the applications testing. The task force issued a data call to gather a list of the applications used in NOAA. The list was then divided into three tiers based on mission critically and breadth of deployment. Tier 1 applications, the most critical and widely used, were divided up among the test teams and will be tested in early December. The results will be recorded in CasaNOSA for peer review and shared with NIST, Census, and DOC .

## **Phase III: Deployment**

The implementation will be broken into three areas, Active Directory environments, standalone internal systems, and remote systems and laptops. The three areas can be implemented independently and the precedent for each LO should be based on the availability of resources, risk, and other operational aspects.

### ***User Notification***

It is essential that users are aware of the significant changes affecting NOAA IT. It is recommended that the NOAA CIO issue an all hands memorandum informing employees of this effort prior to any changes being implemented. Appendix B contains the suggested memorandum.

It is also recommend that regular updates be issued to the constituency during the implementation so that disruptions can be minimized and the NOAA mission is not negatively impacted.

### ***Collaboration***

The Secure Configuration Working group will sponsor a collaboration facility to support the system administrators during the deployment of the FDCC. The collaboration facility will be used to share issues, workarounds, and other information regarding the

deployment of the FDCC. The working group will monitor the collaboration facility to help resolve NOAA issues, coordinate with NIST, and resolve any issues that cannot be effectively resolved at the local level. The working group is using the NMFS WebEx WebOffice tools and CasaNOSA for collaboration.

NOAA is also working with NIST and Census to coordinate testing, implementation strategies, and sharing results workarounds and other information.

## ***Implementation***

The implementation strategy will separate NOAA IT resources into three groups active directory environments, standalone internal systems, and remote systems. The approach for each group is documented below. During implementation each group may be addressed in parallel depending on resources.

### **Active Directory Environments**

#### ***Scope***

This section applies to devices managed within and active directory structure. This includes all Windows XP systems regardless of hardware class.

#### ***Strategy***

NOAA Windows Secure Configuration Working Group has agreed to implement the developed and testing NOAA modified Federal Desktop Core Configuration (FDCC) Group Policy Object (GPO) objects using a phased-in approach to limit the overall impact on NOAA IT Systems. NOAA does not operate a single Microsoft Active Directory (AD) Domain, but in fact NOAA operates a multitude of Active Directory Domains throughout the Line Offices.

A phased approach will allow the individual AD administrators to determine the most effective approach for their domain. Four options are listed below with the critical considerations for each option.

Option 1: Organization Specific: Develop a phased approach based on the technical issues specific to the organization's environment.

- FDCC setting that match default XP/Vista Settings
- Require user adjustment, but no negative impact
- Require configuration on other infrastructure
- Require upgrades for most computers
- Require coordination with external IT departments

Option 2: Use the default Microsoft break down to divide settings/risk

- Account Policies

- Password Policies
- Audit Policies
- Event Logs
- System Services
- Domain level settings
- Registry Settings
- User Rights Assignments
- Security Options
- Internet Explorer
- Firewall

Option 3: Computer Role: Deploy the GPOS based on computer roles and postpone problem-settings identified during testing.

- Basic Operations Workstation
- IT-Administrator Workstation
- Developer Workstation
- Scientific Program Workstation
- Manager/VIP Workstations
- Small to Medium to Large population OU(S)

Option 4: Use a combination of any of the above:

- Computer Role approach PLUS Organization Specific
- Computer Role approach PLUS Microsoft Breakdown
- Microsoft Breakdown PLUS Organization Specific

Once an option is selected the AD administrators can use the NIST provided GPO file to create the individual phase GPO files. The phase GPO files can then be tested and applied to the domain according to the LO schedule.

## **Standalone Internal Systems**

### ***Scope***

The deployment method for systems that are not on Active Directory (AD) has to take into account three key requirements: 1. The method must support systems that are networked but not managed by AD as well as systems that are mostly or completely off the network such as travel laptops and remote site machines; 2. The method must depend only on resources that are available to a stock Windows XP Professional system because we cannot assume that any third-party or optional tools will be present in all cases; 3. It is desirable that the method be easily adaptable to automated deployment tools such as Novell ZENworks or Intel LANDesk for sites that have such tools available to them.

The criteria listed above severely restrict the tools that can be used for the deployment.

Since we cannot assume there is a network connection, the FDCC configuration must be deliverable on some kind of removable media such as CDROM or a portable storage device. The desirability of adapting to a desktop management product strongly favors packaging the FDCC updates as a single executable that can be run either manually from the desktop or via an automated tool. Using the tools available on a stock XP machine limits the form of that executable to something any XP machine can use: a Windows script, a DOS style batch file, or a compiled executable written for the purpose. In the case of a script or batch file, any external commands required by the script must be provided as part of the deployment package to ensure their availability.

### ***Strategy***

Working out a reliable method of deployment depends on defining first exactly what changes need to be made to make a workstation FDCC compliant. The NIST FDCC documentation version 1.01 dated 10/30/2007 (<http://fdcc.nist.gov/FDCC-SCAP-Content-Test-v1-0-1.xls>) lists 229 specific configuration settings for an FDCC workstation, 204 of which apply to Windows XP. While some of these settings are the Windows defaults and others may well have already been set by users or administrators, in order to ensure compliance all of the settings should be treated as changes that must be made to every machine. The settings can be divided into two groups, registry settings and security settings/file permissions.

### ***Group 1 Registry Settings***

The majority of FDCC mandated settings are stored in the Windows registry. A full list of these settings in the form of a registry export (REG) file, which is a Microsoft format used for import and export by the REGEDIT utility will be available on the NOAA FDCC Website. The REG format is the most convenient means for defining these settings in a non-AD Environment because it can be directly imported into the registry via REGEDIT with a simple command:

```
REGEDIT /s <filename>
```

The primary caveat here is that the user account running that command has to have Administrator equivalent rights on the workstation. If an admin or support tech is doing the deployment this should be a non-issue. In the case of a deployment package intended for use by a non-admin user, the RUNAS command and an administrative login will be necessary, which raises serious security concerns.

### ***Group 2 Security Settings and File Permissions***

As Windows has evolved Microsoft has chosen to implement newer security controls outside of the registry. As a result some FDCC settings cannot be enforced simply by changing registry values. In an AD environment this is unimportant because the GPO includes these settings along with registry changes. For a standalone system, however, the GPO route is not available. Fortunately there is a method of enforcing these settings that does not require AD or a GPO: security templates. A security template is a text file in Microsoft INF format that specifies security settings to be applied to a machine's local security database. This database contains a number of registry settings but also includes the ability to specify user rights and restrictions, set file system permissions for files and

folders, and enforce Microsoft provided security settings that are not included in the registry. A security template can be applied to a workstation from the command line using the SECEDIT utility, which is included on all Windows XP workstations. A likely command would be:

```
SECEDIT /CONFIGURE /DB secedit.sdb /CFG <INF file> /OVERWRITE /QUIET
```

As with REGEDIT, this would require administrative privileges to the workstation.

### ***Packaging for Deployment***

At its most basic, a deployment package for FDCC compliance would consist of:

- An FDCC.REG file containing the registry changes
- An FDCC.INI security template
- REGEDIT.EXE (in case it has been removed from the workstation)
- SECEDIT.EXE (in case it has been removed from the workstation)

These files could be provided on a CDROM to prevent accidental changes. An administrator or support tech could then log into the machine with admin rights, insert the CD, and type in the two command lines needed to deploy the settings to the workstation. This is clearly undesirable for a number of reasons: manually typing command lines is tedious and error prone and this basic method provides no reporting of results.

Encapsulating the commands into a standard DOS/Windows style batch file eliminates the typing problem but does nothing for reporting. A better solution is to develop a script that can apply more intelligence to the process and report on its results. Every Windows XP workstation comes with the Windows Scripting Host (WSH) not only enabled but protected by Windows File Protection against deletion, so the obvious choice for developing the script is to use VBscript and execute it via WSH. A fully developed VBscript for FDCC deployment should meet several feature requirements:

1. Run from removable media, either CD or USB device, or a network path if available.
2. Report in plain text on the process, identifying at minimum the machine name, date and time, success or failure of each step (registry and security template), and any error information returned by REGEDIT or SECEDIT during the process.
3. Ability to direct output report to a local file or network path if available.
4. Allow for simple customization by each line office to specify local variables such as a network path for reporting.

Appendix C contains such a script, tested for use on a standard XP (Professional SP2) workstation. Local settings, including the locations of key executables and data files as well as the logging destination, are placed at the top of the script and clearly labeled to allow localization for each site. The default settings will work as is if the script is run from writable removable media, such as a USB drive or floppy disk, or from a network path. The script reports results to a designated text file in CSV format suitable for importing into a spreadsheet or better tracking tool. The script must be run by a user with Administrator privileges on the machine.

## Remote Systems

This section specifically deals with NOAA Remote Computers and its implementation plan to meet specified schedule outlined on this policy.

### *Scope*

NOAA Remote Computers are defined as any device that is under the Department of Commerce NOAA property and is administered and managed by a NOAA IT department. NOAA Remote Computers (NRC) are divided into two groups: Laptops and PC's.

Laptops are mobile devices used for travel or off-site work purposes. Laptops with Windows XP operating systems and are not part of an Active Directory (AD) structure round up this group.

PC's, defined under this scope, are normally used by a NOAA employee at his/her residence for NOAA-related work. They must have a Windows XP operating system and is also not part of an Active Directory structure.

If any Windows XP NOAA Remote Computer is part of an AD environment, please refer to the Active Directory Implementation Plan subsection.

### *Strategy*

The scripts and tools developed for the Standalone Internal Systems will be used to enforce the FDCC settings on NRC devices. Each line office will be responsible for pushing these scripts locally to their appropriate NRC devices. The scripts must be run locally on each device by the appropriate systems administrator therefore all devices must be physically accessible. This may require remote devices to be returned to NOAA. This can be accomplished during regularly schedule system maintenance activities provided that all devices can be completed in accordance with the schedule below.

### *Schedule*

The following table was derived from the DOC data call of November 14, 2007. Each Line Office provided the following data and the NOAA OCIO will track progress toward this goal.

The columns are defined as:

- LO: Line Office
- No. XP: Number of applicable Microsoft Windows XP computes in your LO.
- NO. FDCC: Number of applicable Microsoft Windows XP computers in your LO that have been configured in accordance with the FDCC and have any exceptions documented in an approved waiver.

<b>FDCC Implementaiton Status actual for 11/1/2007</b>			
<b>LO</b>	<b>No. XP</b>	<b>No. FDCC</b>	<b>%complete</b>
NOS	3521	0	0%
OAR	1665	0	0%
NESDIS	1364	93	7%
NWS	6555	0	0%
OMAO	923	0	0%
NMFS	4259	0	0%
OCIO	1452	0	0%
<b>Total</b>	<b>19739</b>	<b>93</b>	<b>0%</b>

<b>FDCC Implementaiton Status planned for 2/1/2008</b>			
<b>LO</b>	<b>No. XP</b>	<b>No. FDCC</b>	<b>%complete</b>
NOS	3521	2999	85%
OAR	1665	200	12%
NESDIS	1376	1010	73%
NWS	6600	4950	75%
OMAO	930	930	100%
NMFS	4829	4829	100%
OCIO	1452	1452	100%
<b>Total</b>	<b>20373</b>	<b>16370</b>	<b>80%</b>

<b>FDCC Implementaiton Status planned for 4/1/2008</b>			
<b>LO</b>	<b>No. XP</b>	<b>No. FDCC</b>	<b>%complete</b>
NOS	3521	2999	85%
OAR	1665	200	12%
NESDIS	1376	1010	73%
NWS	6600	4950	75%
OMAO	930	930	100%
NMFS	4829	4829	100%
OCIO	1452	1452	100%
<b>Total</b>	<b>20373</b>	<b>16370</b>	<b>80%</b>

<b>FDCC Implementaiton Status planned for 8/1/2008</b>			
<b>LO</b>	<b>No. XP</b>	<b>No. FDCC</b>	<b>%complete</b>
NOS	3521	3521	100%
OAR	1665	1665	100%
NESDIS	1376	1376	100%
NWS	6600	6600	100%
OMAO	930	930	100%
NMFS	4829	4829	100%
OCIO	1452	1452	100%
<b>Total</b>	<b>20373</b>	<b>20373</b>	<b>100%</b>

## **Reporting**

It is critical to accurately report the progress being made during the implementation phase. Each line/staff office is required to report their progress bi-weekly to the NOAA CIO. A progress report template has been created and must be used for all reporting. Status reports are due COB on the following days:

12/31/2007  
1/14/2008  
1/28/2008  
2/1/2008  
2/11/2008  
2/25/2008  
4/1/2008  
8/1/2008

After the February 25 report is complete the CIO Council will determine the additional reporting requirements.

## **Phase IV: Monitoring and Compliance**

Compliance Monitoring:

OMB has also required that automated SCAP tools be used to implement, report, and ensure FDCC compliance. NOAA currently own Secure Elements C5EVM, one of the primary tools supporting the NIST SCAP program. Additional work needs to be done to determine if Secure Elements is appropriate for NOAA to use for compliance monitoring and reporting. NOAA also owns Lumension (formally Harris STAT) Vulnerability Scanner which is currently developing SCAP capabilities with an expected delivery date of February 2008. The Lumension tool is not included in the current products licensed by NOAA. NOAA would incur a cost of approximately \$5.00 per target system to license the Lumension tool. A third tool to consider is adding capabilities to McAfee Total Protection Suite to support policy compliance.

NOAA LOs should also consider methodologies to cross reference the SCAP compliance scans with the original FDCC target list and the Sunflower Asset tool.

## **Waivers**

Until otherwise notified by DOC, OMB, or NIST we will operate under the guidance provided in the NOAA Secure Configuration for Windows Policy (NISN 4.001) as stated below.

In the event that compliance with this policy is not possible or practical, offices may apply for a waiver of one or more requirements of this policy. The waiver

request must be fully justified and supported by the organization's Chief Information Officer (CIO). Waivers may apply to a defined class of personal computers and/or laptops. The waiver may be in memorandum format, and must provide the following information:

- 1) A brief rationale for non-compliance with the NOAA standard desktop configuration;
- 2) A brief statement of the adverse impact or risk of implementing the NOAA standard desktop configurations on critical business processes and IT resources;
- 3) Identification of any impacts on other NOAA critical business processes, including those of outside agencies and third parties;
- 4) For class waivers, include a concise description of the scope of personal computers and/or laptops included within the waiver request, and
- 5) Projected date for compliance.

The NOAA CIO will make the final approval for all waiver requests.

# Appendix A - ITSC Working Group and Task Force Charters

## ***NOAA IT Security Committee Working Group Terms of Reference***

### **Working Group Name:**

NOAA Windows Secure Configuration Working Group (NWSC-WG)

### **Purpose:**

The NWSC-WG will review all applicable policies and guidance related to the establishment of a secure configuration standard for the Windows operating system, combine all relevant controls and settings from guidance sources into a single document, test these controls for compatibility, and then make recommendations to the ITSC regarding their implementation.

The major objective of this group is to test the FDCC and ensure that it can be implemented per OMB and NOAA directives identify issues with implementation, and make recommendations on how best to address any issues found.

### **Tasks:**

The tasks of this working group are to:

- (1) Identify and document all applicable policies and guidance related to the establishment of a secure configuration standard for the Windows operating system for the NOAA environment. This will be based off the FDCC, but should also incorporate DOC and NOAA requirements.
  - a. Determine which configuration settings should augment FDCC based on other policies, guidance, and best practices.
  - b. ITSC approval required for non-FDCC configuration settings, which should be only a few, if any.
  - c. This item is time sensitive, as everything else is dependent upon it.
- (2) Review all Applicable Configuration Settings
  - a. Review each configuration setting to determine if it is appropriate to the NOAA operational environment.
  - b. Thoroughly documenting any recommended exceptions.
  - c. Final product will be .xccdf content.
- (3) Test each control for compatibility with existing NOAA applications.
  - a. Develop formal test and user acceptance procedures and documentation

- b. Test common COTS and GOTS used by NOAA
  - c. Test Line Office specific applications
  - d. Request field offices test other software not specified above
- (4) Present findings and recommendations to the NOAA IT Security Committee.
- a. Detailed controls list, by source, including settings, and recommended exceptions if any.
  - b. Controls which cannot be adopted immediately, and alternatives to remediate.
  - c. Maintain an inventory of FDCC-incompatible applications and their owners.
- (5) Develop a recommend implementation plan with completion milestones for locations with and without Active Directory.
- (6) Determine follow-on actions, including but not limited to:
- a. Continuous monitoring of the FDCC configuration.
  - b. Develop general strategy to address other operating systems (Mac, Linux, Solaris, Cisco IOS, etc.) based on lessons learned from Windows FDCC implementation.

**Membership:**

Chair: Stefan Leeb  
 Co Chair: Larry Reed

**Members:**

Membership shall include one Technical and one Policy representative from each line office and NOAA OCIO.

Stefan Leeb	NMFS	Policy
Rick Rubio	NMFS	Technical
John D. Parker	NOS	Policy
Thomas K. Murphy	NOS	Technical
Vincent Garcia	OAR	Policy
TBD	OAR	Technical
Greg Bass	OMAO	Policy
Ray Mitchell	OMAO	Technical
Wayne Zahn	OMAO	Technical Alt
Harry Tabak	NWS	Policy
Steve Schild	NWS	Technical
Charles MacFarland	NESDIS	Policy
Ron Charette	NESDIS	Technical
David Hennessey	OCIO	Policy
Reze Latifzadeh	OCIO	Technical

**Roles and Responsibilities:**

**Chair:** The chair is responsible for coordinating the working group activities. The chair will determine the necessary resources to accomplish the goals described herein. The chair shall provide status updates to the ITSC at every meeting.

**Members:** The working group members must commit, with their supervisors knowledge and approval, to provide the service necessary to complete the task of the working group.

**Decision Making Process:**

The working group will use the decision making process described in the ITSC terms of reference. All decisions made by the chair without full consensus of the membership must be reported to the ITSC in the next status update.

**Charter:**

- Created by the ITSC on September 26, 2007.
- The mission of this subcommittee will be reevaluated during the first ITSC meeting in February 2008.)
- Requirements
  - OMB M-07-11
  - NOAA Secure Configuration for Windows Policy

**Authority:**

This subcommittee was authorized by the NOAA Information Technology Security Council on September 26, 2007

**Schedule and Deliverables:**

The following table defines the schedule and deliverables for this working group, along with other relevant dates.

<b>Deliverables and Milestones</b>	<b>Due Date</b>
NWSC-WG provides ITSC members: - Configuration settings list along with GPO and .inf - Applications list to be tested - Draft implementation plan	October 15, 2007
ITSC Meeting - ITSC approves: - Draft implementation plan - Configuration settings list - Applications to be tested. Testing commences.	October 17, 2007
ITSC Reports to CIO's – Draft Implementation plan	October 23, 2007
ITSC Meeting – Final test results reported	November 28, 2007

**Resources:**

NMFS is providing a collaboration portal which will be made available to the ITSC and all testers, which will be located at <https://nscwg.noaa.webexone.com/>

DRAFT

## **TASK FORCE – IMPLEMENTATION**

### **Mission/Objectives:**

Develop implementation plan with completion milestones for locations with and without active directory. Include technical recommendations on how non-AD sites might implement.

All documents, drafts and final, should be stored on Work Force portal in the “Implementation Task Force Documents” folder.

### **Initial Milestones:**

October 10 – Draft implementation plan due at 9am for Work Group review

October 15 – Final draft due at NOON for Work Group vote

### **References:**

Draft NOAA Implementation Plan, dated 4/22/07

DOC Implementing Commonly Accepted Security Configurations for XP, dated 5/1/07

NOAA Comments/Responses to DOC document

NOAA IT Security Committee Working Group Terms of Reference for NWSC-WG

### **First Meeting Agenda:**

1. Choose Task Force Leader
2. Document Task Force Membership and contact info
3. Review Task Force objectives
4. Discuss and agree upon approach
5. Work on objectives
6. Create list of Action Items, due dates, and responsible parties
7. Schedule additional meetings if necessary

### **Membership:**

<b>Name</b>	<b>Org</b>	<b>Telephone</b>
Larry Reed ( Leader )	NOAA OCIO	(301) 713-0042 x 218
John D. Parker	NOS	(301) 713-1156 x 174
Laura Gutierrez	NMFS	(301) 713-2319 x 130
Dave Hennessey	NOAA OCIO	(301) 713-0042 x 207
John Dandy	NOS	(301) 713-1156 x 175
Michael Raugh	NESDIS	(301) 713-0519
Vincent Garcia	OAR	(301) 713-1109
Carlton Parks	NESDIS	(301) 713-1139

## **TASK FORCE – CONFIGURATION**

### **Mission/Objectives:**

- (1) Identify and document all applicable policies and guidance related to the establishment of a secure configuration standard for the Windows operating system for the NOAA environment.
  - a. FDCC mandated configuration settings
  - b. DOC mandated differences
  - c. NOAA mandated differences
  - d. Other differences based on other policies, guidance, and best practices.
  
- (2) Review all identified Configuration Settings
  - a. Review each configuration setting to determine if it is appropriate to the NOAA operational environment
  - b. Thoroughly document any recommended exceptions
  - c. Final configuration settings will be converted into .xccdf content to be used by compliance checking tool
  
- (3) When application testing concludes document findings and recommendations based on those test results.
  - a. Detailed controls list, by source, including settings, and recommended exceptions if any.
  - b. Controls which cannot be adopted immediately, and alternatives to remediate.
  - c. Maintain an inventory of FDCC-incompatible applications and their owners.

All documents, drafts and final, should be stored on Work Force portal in the “Configuration Task Force Documents” folder.

### **Initial Milestones:**

October 10 – Draft configuration settings list due at 9am for Work Group review  
October 15 – Final configuration settings list due at NOON for Work Group vote  
November 21 – Final recommendations based on test findings due for Work Group vote

### **References:**

DOC Security Plan  
NOAA Security Plan  
Federal Desktop Core Configuration (FDCC)  
NIST SP800-53A  
NOAA IT Security Committee Working Group Terms of Reference for NWSC-WG

**First Meeting Agenda:**

8. Choose Task Force Leader
9. Document Task Force Membership and contact info
10. Review Task Force objectives, ensuring consistency with WG TOR
11. Discuss and agree upon approach
12. Work on objectives
13. Create list of Action Items, due dates, and responsible parties
14. Schedule additional meetings if necessary

DRAFT

## Appendix B - NOAA All Hands Memorandum

MEMORANDUM FOR: ALL NOAA Personnel

FROM: Joseph F. Klimavicz  
Chief Information Officer  
National Oceanic and Atmospheric Administration

SUBJECT: Federal Desktop Core Configuration

### A MESSAGE FROM THE NOAA CIO

The Office of Management and Budget has mandated that all federal agencies implement the Federal Desktop Core Configuration (FDCC) on Microsoft Windows XP and VISTA computers by February 1, 2008. The FDCC is a standard set of security configurations for all computers running these operating systems.

The goal of FDCC is to improve information security and reduce operating costs. The challenge for NOAA, and all federal agencies, is to ensure compliance while maintaining full functionality of all required computer application programs.

To meet this challenge, NOAA has formed the NOAA Windows Secure Configuration Working Group (NWSC-WG). IT Security Officers and technical representatives from each NOAA Line Office are meeting weekly to develop test and implementation plans that will bring NOAA into compliance.

Each Line Office will determine its own FDCC implementation schedule. Your Line Office IT Security Officer or Help Desk personnel will notify you of the implementation schedule and pending changes to your computers.

Please visit the following web site for more information: <https://www.csp.noaa.gov/noaa/security-program/fdcc/>

## Appendix D - VB Script for standalone systems

```
'=====
' FDCCdeploy.vbs -- VBscript to deploy the FDCC configuration settings
'   to an XP workstation.
'
' Prepared by Michael Raugh, NOAA/NESDIS (michael.raugh@noaa.gov)
'   for the NOAA Secure Configuration Working Group
'   November 2007
'
' For best results execute using CSCSCRIPT.EXE
'=====
' LOCAL SETTINGS
'
' Modify these text strings to fit your environment
' Either mapped drives or UNC pathnames will work on a network
' If you don't specify a full path (ie, X:\FDCCstuff\filename) the script
' will use the directory in which FDCCdeploy.vbs sits (which would be ideal
' for working from removable media).
'
' REG_FILE_NAME is the full pathname of the registry settings file
Const REG_FILE_NAME = "FDCC.REG"
'
' TEMPLATE_FILE_NAME is the full pathname of the security template file
Const TEMPLATE_FILE_NAME = "FDCC.INF"
'
' LOG_FILE_NAME is the full pathname of the log file to use.
Const LOG_FILE_NAME = "DEPLOY.LOG"
'
' Commands we'll be invoking. You shouldn't need to edit these unless there's
' something strange in your environment (like these files are not in the path).
Const RegEditExecPath = "regedit.exe"
Const SecEditExecPath = "secedit.exe"
'-----
' End of local settings
' Don't change anything below here unless you know your VBscript
'-----

'Handy objects needed at various points
Dim oMachInfo, oFileSys, oShell
Set oMachInfo = CreateObject("WScript.Network")
Set oFileSys = CreateObject("Scripting.FileSystemObject")
Set oShell = CreateObject("WScript.Shell")

'-----
' STEP ONE: Construct and execute the command to import registry settings
'-----

Dim RegEditCmd, objExec, RegEditResult

RegEditCmd = RegEditExecPath & " /s " & REG_FILE_NAME
WScript.Echo(" - Executing: " & RegEditCmd)

Set objExec = oShell.Exec(RegEditCmd)

'Wait for the command to complete
```

```

Do
  WScript.Sleep(200)
Loop Until objExec.Status = 1

'REGEDIT always returns success, so we need to test for an actual
'change to be sure it worked. I slipped in a specific entry to
'test for: HKEY_LOCAL_MACHINE\Software\FDCC\FDCCversion.
'(This could be handy later for verifying that FDCC was deployed)
Dim FDCCkey
FDCCkey = "HKLM\Software\FDCC\FDCCversion"
If oShell.RegRead(FDCCkey) = "1.0.1" Then
  WScript.Echo("  Registry import successful")
  RegEditResult = "Success"
Else
  WScript.Echo("  Registry import FAILED!")
  RegEditResult = "Failure (no return code)"
End If

'-----
' STEP TWO: Construct and execute the command to import the security template
'-----
Dim SecEditCmd, SecEditResult

SecEditCmd = SecEditExecPath & " /CONFIGURE /DB secedit.sdb " & _
"/CFG " & TEMPLATE_FILE_NAME & " /OVERWRITE /QUIET"
WScript.Echo(" - Executing: " & SecEditCmd)

Set objExec = oShell.Exec(SecEditCmd)
Do
  WScript.Sleep(200)
Loop Until objExec.Status = 1

'SECEDIT does return nonzero on failure, so we can use that output.
If objExec.ExitCode <> 0 Then
  SecEditResult = ""Failure: " & objExec.StdErrReadAll & ""
  WScript.Echo(" " & SecEditResult)
Else
  WScript.Echo("  Security template imported")
  SecEditResult = "Success"
End If

'-----
' STEP THREE: Compose the log report as a single line in CSV format and
' write that to the log file.
'-----
WScript.Echo(" - Logging results to " & LOG_FILE_NAME)

Dim timestamp, logline, ThisPCName
ThisPCName = oMachInfo.ComputerName

' Log format: ComputerName,Date and Time,REGEDIT results,SECDIT results <CRLF>
timestamp = FormatDateTime(Now(),vbShortDate) & " " &
FormatDateTime(Now(),vbShortTime)
logline = ThisPCName & "," & timestamp & "," & RegEditResult & "," & SecEditResult
& vbCrLf

'Open the log file. Create a new one if it doesn't already exist
Dim oLogFile
Set oLogFile = oFileSys.OpenTextFile(LOG_FILE_NAME,8,True)

'Write the single line log entry
oLogFile.WriteLine(logline)

```

```
'and close the file again to be a good citizen
oLogFile.Close

If (RegEditResult = "Success" And SecEditResult = "Success") Then
    WScript.Echo(vbCrLf & "FDCC configuration deployed" & vbCrLf)
Else
    WScript.Echo(vbCrLf & "Errors occurred during deployment -- see " & LOG_FILE_NAME
& vbCrLf)
End If
```

DRAFT