



# MSHA NETWORK NEWS

Volume 4, Issue 1

keeping you connected

April 2009

## MSHA IMPLEMENTS THE FEDERAL DESKTOP CORE CONFIGURATION

In March 2007, the *Office of Management and Budget* (OMB) published a memorandum (M-07-11) regarding the "Implementation of Commonly Accepted Security Configurations for *Windows*® Operating Systems."

This memorandum directed agencies with *Windows XP*® deployed and/or planning to upgrade to the *Vista*® operating system to adopt the *Federal Desktop Core Configuration* (FDCC) security configurations developed by the *National Institute of Standards and Technology* (NIST), the *Department of Defense* (DOD), and the *Department*

*of Homeland Security* (DHS).

After the initial OMB memorandum, NIST published the first version of the FDCC in July 2007. After review and comment, NIST published an updated version of the FDCC in June 2008.

MSHA must now implement the FDCC security settings as mandated by OMB in a second memorandum (M-08-22) issued in August 2008.

All Federal Agencies must comply, and any deviations must be thoroughly documented and approved.

Changes to the FDCC will pass through the

FDCC *Change Control Board* (CCB) portion of the *Technology Infrastructure Subcommittee* (TIS).

The TIS subcommittee, created with the release of the FDCC, convenes under the *Federal Chief Information Officer* (CIO) Council's *Architecture and Infrastructure Committee* (AIC).

The TIS must approve any changes to the FDCC settings.



## WHY SHOULD I CARE?

- The security changes to *Windows XP* settings will affect your MSHA **desktop** and **laptop** computers.
- The PEIR Network Team is making every effort to keep you informed while we prepare for the transition to using the FDCC security settings on our MSHA core loads.
- As soon as PEIR determines what the specific impacts are, we will advise you promptly.

## HOW WILL THIS AFFECT MY COMPUTER?

The FDCC security settings will affect **ALL** MSHA desktop and laptop computers.

PEIR has been testing the settings and working with the *Information Security Office* (ISO) for several months to determine the impact to MSHA's workforce.

We have been changing items that can be changed and requesting exceptions for those that cannot be changed because the impact to our daily

business is too great.

Please be aware that this change affects only MSHA desktop and laptop computers.

It does not affect our servers (W, local T and H drives) and it does not affect laboratory computers, such as those in Pittsburgh and Triadelphia.

Some of the impacts include:

- **Log On Information**  
Log on information will

NOT be saved. You will have to enter your MSHA network User ID and Password each time you log on.

- **Wireless**  
Wireless access may be impacted if you try to use a non-MSHA wireless card.



## NEED HELP?

WE'RE HERE TO HELP!

MSHA HELP  
DESK

1-877-778-6055

MONDAY —  
FRIDAY

7 AM TO 8 PM  
EASTERN TIME

## HOW WILL THIS AFFECT MY COMPUTER? (CONT'D)



**FDCC WILL AFFECT ALL MSHA DESKTOP AND LAPTOP COMPUTERS**

Windows® wireless automatic configuration will be turned off.

- **Local Administrator Privileges**  
Those with local administrative privileges may lose them unless granted an exception.
- **Local Administrator Account**  
If you are granted an exemption for local administrative privileges, IT support will provide you with an administrative account in addition to your regular account.

The administrative account is for installing software and running applications that require it. Your user account is for e-mail, accessing the Internet, and running applications.

The user account must be used for day-to-day op-

erations.

- **Special Software**  
If you have special software loaded on your computer, it may not function properly.

The network team is working to identify special software and test it with the FDCC configuration.

- **Lab Computers**  
The MSHA laboratories in Pittsburgh and Triadelphia run scientific computers.

Specialized computers, such as these, used primarily for scientific efforts like running software and collecting data from scientific equipment, are **exempt** from the FDCC settings.

These systems, however, must still be securely protected by other

means, such as removing e-mail and Web browser software, keeping the computer on a local “subnet” rather than on the main network, and other controls.

Also, these special purpose computers that are exempt from FDCC still must be tracked and documented.

The MSHA network team is working to document our scientific computers systems and how they are secured for FDCC compliance.

- **Used by a Scientist**  
A computer used by a scientist, but that is used primarily for e-mail access, Web browsing, and non-scientific use **is** included under the FDCC security regulations and must adhere to those security settings.

## WHAT ABOUT EXEMPTIONS?

**SCRs MUST BE FILED FOR ANY NEW SOFTWARE OR HARDWARE THAT WILL BE ON THE MSHA NETWORK.**

Once the FDCC security settings are in place, the only way to change them is to apply to **DOL** for an exemption.

DOL will authorize exemptions only if there are technology restrictions, such as legacy systems, or when implementing the FDCC control would **significantly impact** the

Agency's **ability to meet its mission.**

Therefore, those wanting exemptions for **NEW** software or hardware must go through the *System Change Request* (SCR) process.

The SCR form is located on the MSHA intranet page in the PEIR Program Area: <http://mshanet.msha.gov/>

[ProgArea/PEIR/PEIR-home.asp](#)

Scroll down to the bottom of the page and click the **“Configuration Management System Change Request”** link.

Fill out the form and submit it for any new changes to your computer.

## HAVE OTHER AGENCIES IMPLEMENTED FDCC?

**Yes.**

Several other Federal agencies have already implemented FDCC, including the *National Institutes of Health* (NIH), the *National Cancer Institute* (NCI), the *National Security Agency* (NSA), and the *Department of Homeland Security* (DHS).

The *National Institute of Stan-*

*dards and Technology* (NIST) worked with several agencies on the FDCC standards (see below) for *Windows XP*® and *Windows Vista*® operating systems.

NIST does not endorse the use of any particular product or system, and is not mandating the use of the *Windows XP*® or *Vista*® operating systems. Nor is NIST establish-

ing conditions or prerequisites for Federal agency procurement or deployment of any system.

NIST is not precluding any Federal agency from procuring or deploying other computer hardware or software for which NIST has not developed a publication, security configuration checklist, or virtual testing environment.



## HOW WAS FDCC CREATED?

The *Windows Vista*® FDCC is based on DOD customization of the Microsoft Security Guides for both *Windows*® *Vista*® and *Internet Explorer*® 7.0.

Microsoft's *Vista*® Security Guide was produced through a collaborative effort with *Defense Information Systems Agency* (DISA), *National Security Agency* (NSA), and *National Institute of Standards and Technology* (NIST).

The guide reflects the consen-

sus recommended settings from DISA, NSA, and NIST for the *Windows Vista*® platform.

The *Windows*® *XP*® FDCC is based on Air Force customization of the *Specialized Security-Limited Functionality* (SSLF) recommendations in **NIST SP 800-68** and DOD customization of the recommendations in Microsoft's *Security Guide for Internet Explorer*® 7.0.

NIST is working with a num-

ber of IT vendors on standardizing security settings for a wide variety of IT products and environments.

The NIST process is documented in **NIST SP 800-70 - Security Configuration Checklists Program for IT Products: Guidance for Checklists Users and Developers.**



**MSHA WILL IMPLEMENT FDCC IN SUCH A WAY SO THAT YOU WON'T HAVE TO DO ANYTHING!**

## WHEN WILL MSHA IMPLEMENT FDCC?

As soon as we have a date, we will inform you so that you can prepare for the changes implementing FDCC will bring.

You will not have to do anything to your computer — the MSHA Network Team will be implementing FDCC using the capabilities of the

*Windows*® servers.

In the meantime, if you have any questions, you may contact the **MSHA Help Desk.**

### NEED HELP?

**WE'RE HERE TO HELP!**

**MSHA HELP DESK**

**1-877-778-6055**

**MONDAY — FRIDAY**

**7 AM TO 8 PM EASTERN TIME**



Previous editions of *Network News* covering [Remote Access](#), [Point-sec](#), and [Two-Factor Authentication](#) are available.

**Click the links to go!**



A publication from PEIR  
Program Evaluation and  
Information Resources

A division of the **Mine Safety & Health  
Administration**

**Major offices:**

Arlington, VA  
Beckley, WV  
Lakewood, CO  
Pittsburgh, PA  
Triadelphia, WV

**MSHA.GOV**

**MSHANET.MSHA.GOV**

**PROTECTING MINERS' SAFETY  
AND HEALTH SINCE 1978**



## MSHA MISSION

To eliminate fatal mining accidents and to reduce the frequency and severity of non-fatal accidents; to minimize health hazards; and to promote the improved safety and health conditions in the Nation's mines by administering the provisions of the  
**Federal Mine Safety and Health Act of 1977.**

## MSHA'S HISTORY

Although the **Federal Mine Safety and Health Act of 1977** moved mine monitoring to the Department of Labor and gave the agency, MSHA, its name, the history of regulation in the mining industry stretches back to 1865 and the creation of a Federal mine bureau.

In 1910, congress established the **Bureau of Mines** in the Department of Interior. The Bureau of Mines was denied the ability to inspect or supervise mines.

In 1952, Congress passed the **Federal Coal Mine Safety Act**, providing for annual inspections of underground coal mines and setting mandatory safety standards for gassy mines.

In 1963, a Federal Task Force formed to investigate mine safety and recommend improvements.

In 1966, the **Federal Metal and Nonmetallic Mine Safety Act** became law, partially in response to the Task Force findings.

Congress responded to the Task Force findings in with the **Federal Coal Mine Health and Safety Act of 1969**. For the first time, binding safety and health standards for the US coal industry were established and operators and miners were required to comply.

Inspections would now take place quarterly along with providing assistance to states in enforcing coal mine health and safety programs. It also

provided protection for whistleblowers and established a compensation plan for "black lung" along with sampling of coal mine dust and vigorous new dust standards.

Implementation was not easy and there were still too many deaths and injuries.

Congress reacted in 1976 with a review of the enforcement of the **1966 Metal Act** and the **1969 Coal Act**.

In **1977**, Congress gave us the **Federal Mine Safety and Health Act**. This Act provided for the creation of a Mine Safety and Health Administration. MSHA was created under the Department of Labor on **March 9, 1978** to administer a broad regulatory program to reduce injuries, illness, and fatalities in mining.