Report No. DODIG-2012-050 February 3, 2012

Inspector General
United States Department of Defense

Improvements Needed With Host-Based Intrusion Detection Systems

Warning
"This report is a product of the Inspector General of the Department of Defense. Its contents shall not be disclosed to any individual within the Department of Defense who does not have a valid need for such access in connection with the accomplishment of a lawful and authorized Government purpose. Release outside the Defense Department requires approval of the Inspector General."

Additional Copies

To obtain additional copies of this report, contact the Secondary Reports Distribution Unit at (703) 604-8937 (DSN 664-8937) or fax (571) 372-7469.

Suggestions for Audits

To suggest or request audits, contact the Office of the Deputy Inspector General for Auditing by phone (703) 604-9142 (DSN 664-9142), by fax (571) 372-7469, or by mail:

Department of Defense Office of Inspector General
Office of the Deputy Inspector General for Auditing
ATTN: Audit Suggestions/13F25-04
4800 Mark Center Drive
Alexandria, VA 22350-1500

Acronyms and Abbreviations

CNCI	Comprehensive National Cybersecurity Initiative
DISA	Defense Information Systems Agency
DMEA	Defense Microelectronics Activity
FHP&R	Force Health Protection and Readiness
FISMA	Federal Information Security Management Act
FRAGO	Fragmentary Order
HBSS	Host Based Security System
HIDS	Host-based Intrusion Detection System
HIPS	Host Intrusion Prevention System
IDS	Intrusion Detection System
JTF-GNO	Joint Task Force–Global Network Operations
NIPRNet	Unclassified but Sensitive Internet Protocol Router Network
SIPRNet	Secret Internet Protocol Router Network
USCYBERCOM	U. S. Cyber Command

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
4800 MARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22350-1500

February 3, 2012

MEMORANDUM FOR DOD CHIEF INFORMATION OFFICER
COMMANDER, U.S. CYBER COMMAND
DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY
DIRECTOR, FORCE HEALTH PROTECTION AND READINESS
DIRECTOR, DEFENSE MICROELECTRONICS ACTIVITY

SUBJECT: Improvements Needed With Host-Based Intrusion Detection Systems (Report No. DODIG-2012-050)

We are providing this final report for your information and use. DoD Components did not consistently use host-based intrusion detection systems to detect, report, and mitigate cyber intrusions. Given this, DoD computer systems may encounter unauthorized access to sensitive data, and U.S. Cyber Command may not fully identify trends on intrusions. We considered management comments on a draft of this report when preparing the final report. Management comments conformed to the requirements of DoD Directive 7650.3. Therefore, additional comments are not required.

We appreciate the courtesies extended to the staff. Please direct questions to (b) (6) at (703) 604-(b) (6) (DSN 664-(b) (6)

(b) (6)

Alice F. Carey
Assistant Inspector General
Readiness, Operations, and Support

~~Warning~~

~~This report is a product of the Inspector General of the Department of Defense. Its contents shall not be disclosed to any individual within the Department of Defense who does not have a valid need for such access in connection with the accomplishment of a lawful and authorized Government purpose. Release outside the Defense Department requires approval of the Inspector General~~

~~FOR OFFICIAL USE ONLY~~

Report No. DODIG-2012-050 (Project No. D2011-D000LB-0124.000) February 3, 2012

Results in Brief: Improvements Needed With Host-Based Intrusion Detection Systems

What We Did

Our objective was to determine whether DoD, using host-based intrusion detection systems (HIDS), was detecting, reporting, and mitigating cyber intrusions. We reviewed the status of deployment and configuration of HIDS as reported by DoD Components to U.S. Cyber Command, and specifically within the offices of Force Health Protection and Readiness and the Defense Microelectronics Activity. We also reviewed U.S. Cyber Command's ability to monitor intrusions. DoD Components did not consistently use HIDS to detect, report, and mitigate cyber intrusions.

What We Found

~~(FOUO)~~ DoD Components did not install HIDS on 9,148 of 11,268 non-Windows, unclassified computer systems. This occurred because U.S. Cyber Command did not require Components to install HIDS. As a result, DoD non-Windows Unclassified but Sensitive Internet Protocol Router Network (NIPRNet) systems may be at an increased risk to unauthorized activity, such as unauthorized access to sensitive medical information.

~~(FOUO)~~ DoD Components generally installed the McAfee Host Intrusion Prevention System (HIPS) on unclassified, Windows computer systems. However, according to U.S. Cyber Command, DoD Components did not appropriately configure HIPS on 60 percent of DoD's 2.1 million Windows NIPRNet computer systems because personnel believed that the configuration required a large effort. Further, U.S. Cyber Command did not have a reliable method to ensure that DoD Components appropriately configured HIPS. As a result, DoD unclassified computer systems were at an increased risk to unauthorized activity, such as unauthorized access.

~~(FOUO)~~ Additionally, HIPS signatures (which describe security threats and network intrusions) may not have fully addressed DoD-specific threats because U.S. Cyber Command did not review the list of signatures since 2009. As a result, DoD computer systems were at an increased risk to unauthorized activity.

~~(FOUO)~~ Finally, U.S. Cyber Command could not access unclassified, event data from the Host Based Security System because DoD encountered complications when consolidating the unclassified event data from approximately 2.1 million Windows NIPRNet computer systems and DoD focused first on obtaining event data from its secret network. As a result, U.S. Cyber Command may not fully identify cyber intrusion trends across DoD.

What We Recommend

~~(FOUO)~~ Among other recommendations, we recommend the Commander, U.S. Cyber Command, develop a formal plan to deploy HIDS or other comparable security measures to non-Windows computer systems. We also recommend the Director, Defense Information Systems Agency, develop an automated capability for U.S. Cyber Command to determine whether DoD Components are appropriately configuring HIPS.

Management Comments and Our Response

Management comments were responsive and agreed with the recommendations. No further comments are required. See the recommendations table on the back of this page.

Recommendations Table

Management	Recommendations Requiring Comment	No Additional Comments Required
Commander, U.S. Cyber Command		A, B.1, C, D.2
Director, Defense Information Systems Agency		B.2, D.1
Director, Force Health Protection and Readiness		B.3
Director, Defense Microelectronics Activity		B.4

Table of Contents

Table of Contents (cont'd)

Introduction

Objective

Our objective was to determine whether DoD, using host-based intrusion detection systems (HIDS), was detecting, reporting, and mitigating cyber intrusions. We reviewed the status of deployment and configuration of HIDS as reported by DoD Components to U.S. Cyber Command, and specifically within the offices of Force Health Protection and Readiness (FHP&R) and the Defense Microelectronics Activity (DMEA). We also reviewed U.S. Cyber Command's (USCYBERCOM) ability to monitor host-based intrusions. See the appendix for the scope and methodology.

Background

Threats to DoD Networks

The "DoD Strategy for Operating In Cyberspace," July 2011, revealed that many foreign nations were working to exploit DoD unclassified and classified networks, and some foreign intelligence organizations have already acquired the capacity to disrupt elements of DoD's information infrastructure. Moreover, other groups increasingly threaten to penetrate and disrupt DoD networks and systems. Every year, intellectual property larger than the information contained in the Library of Congress is stolen from networks maintained by U.S. businesses, universities, and Government entities. In 2008, DoD suffered a large compromise of its classified and unclassified computer networks because someone attached a flash drive with malicious code, created by a foreign intelligence agency, to a U.S. Central Command network. The code provided an avenue to transfer data out of DoD. The Deputy Secretary of Defense considered this incident the most significant breach of U.S. military information systems.

Use of Intrusion Detection Systems

In January 2008, President George W. Bush launched the Comprehensive National Cybersecurity Initiative (CNCI) in National Security Presidential Directive 54/Homeland Security Presidential Directive 23, which highlights the importance of detecting and preventing intrusions into computer systems. The CNCI consists of a number of initiatives designed to help secure the U.S. in cyberspace. Initiative 2 of the CNCI directs the deployment of Intrusion Detection Systems (IDS) across the Federal enterprise to better identify intrusions. Further, Initiative 3 of the CNCI directs pursuing the deployment of intrusion prevention systems across the Federal enterprise to automatically detect and respond to cyber threats before adverse actions occur.

> *Initiative 2 of the CNCI directs the deployment of Intrusion Detection Systems (IDS) across the Federal enterprise to better identify intrusions.*

~~(FOUO)~~ DoD uses multiple types of IDS to detect intrusions on its networks. Network IDS are installed on segments of the DoD networks and detect suspicious traffic entering the network. Wireless IDS detect inappropriate access to DoD networks through wireless

access points. HIDS are installed on workstations and servers and monitor those systems for network-based attacks and host-specific attacks or events.

Host Based Security System and Host Intrusion Prevention System

DoD selected McAfee's Host Intrusion Prevention System (HIPS) as its HIDS on DoD computer systems, including workstations and servers. HIPS is one of the components of the Host Based Security System (HBSS), a commercial off-the-shelf security product licensed by McAfee to DoD. HBSS is composed of seven components, including the McAfee Agent and HIPS. The McAfee Agent is the initial HBSS component that is installed on computer systems and allows computer systems to send information to HBSS analysts. HIPS acts as a HIDS on computer systems, but can also prevent attacks on the systems. HBSS performs many other functions besides detecting and preventing intrusions. For example, HBSS also includes the Device Control Module, which can be configured to disable the use of flash media or other external devices on computer systems.

HIPS Guidance

~~(FOUO)~~ The Joint Task Force–Global Network Operations (JTF-GNO), now part of USCYBERCOM, issued Fragmentary Order (FRAGO) 13, "Requirements for Rapid Deployment of HBSS on SIPRNet [Secret Internet Protocol Router Network] and Unclassified Networks," in increments from November 26, 2008, through May 23, 2011. FRAGO 13 requires DoD Components to install HIPS on all SIPRNet computer systems and Unclassified but Sensitive Internet Protocol Router Network (NIPRNet) workstations and servers (computer systems) with supported Windows operating systems by October 31, 2009.

HIPS Signatures

FRAGO 13 states that HIPS signatures describe security threats, attack methodologies, and network intrusions. Each signature has a default severity level, which describes the potential danger of attack and falls into one of four categories:

- **High** indicates clearly identifiable security threats or malicious actions and well-identified vulnerabilities.
- **Medium** indicates activity that identifies applications performing functions they were not intended to perform.
- **Low** indicates where activity occurs when applications and system resources are locked and cannot be changed.
- **Information** indicates modification to the system configuration, but is not generally evidence of an attack.

HIPS is designed to detect and prevent worms, Trojan horses, buffer overflow attacks, malformed commands, critical system file modifications, unauthorized access, and privilege escalation.

Review of Internal Controls

~~(FOUO)~~ DoD Instruction 5010.40, "Managers' Internal Control Program (MICP) Procedures," July 29, 2010, requires DoD organizations to implement a comprehensive system of internal controls that provides reasonable assurance that programs are operating as intended and to evaluate the effectiveness of the controls. We determined that internal control weaknesses existed with USCYBERCOM's ability to monitor host-based intrusions. USCYBERCOM personnel did not have a reliable method to ensure that DoD Components appropriately configured HIPS on computer systems within DoD. USCYBERCOM personnel relied on responses from DoD Components to determine whether they configured HIPS in accordance with USCYBERCOM requirements. Also, USCYBERCOM personnel could not access and review NIPRNet HBSS event data because it appropriately focused first on obtaining SIPRNet HBSS event data. We will provide a copy of the report to the senior official responsible for internal controls at USCYBERCOM.

~~(FOUO)~~ Finding A. HIDS Not Required on Non-Windows Computer Systems

~~(FOUO)~~ DoD Components did not install HIDS on 9,148 of 11,268 NIPRNet computer systems with non-Windows operating systems. This occurred because USCYBERCOM did not require Components to install HIDS on computer systems with operating systems other than Windows. Instead, USCYBERCOM focused efforts on computer systems with Windows operating systems because of inherent vulnerabilities with Windows computer systems and approximately 99 percent of DoD computer systems had Windows operating systems. While we agreed with this approach, USCYBERCOM did not develop a formal plan to implement HIDS on non-Windows systems. As a result, DoD non-Windows NIPRNet systems (including those containing medical records) may be at an increased risk of unauthorized activity, such as unauthorized access to sensitive medical information. Also, attacks may go unreported and unmitigated.

~~(FOUO)~~ HIDS Not Installed on Non-Windows Computer Systems

~~(FOUO)~~ Based on data provided by USCYBERCOM, 9,148 of 11,268 non-Windows NIPRNet computer systems did not have HIDS installed. While USCYBERCOM estimated that non-Windows computer systems represented less than 1 percent of the total computer systems on DoD networks, usage of non-Windows computer systems was widespread across DoD. In fact, 34 of 36 DoD Components used non-Windows computer systems, some of which contained sensitive medical records but did not have HIDS installed.

> *(~~FOUO~~) Based on data provided by USCYBERCOM, 9,148 of 11,268 non-Windows NIPRNet computer systems did not have HIDS installed.*

Use of Non-Windows Computer Systems Within DoD

~~(FOUO)~~ According to the FY 2010 Annual Federal Information Security Management Act (FISMA) report, non-Windows operating systems used within DoD included Linux, Solaris, Sun, Hewlett Packard Unix, Macintosh, Advanced Interactive eXecutive, and Berkeley Software Distribution.[1] USCYBERCOM and Defense Information Systems Agency (DISA) personnel could not determine the total number of non-Windows computer systems in DoD. However, according to USCYBERCOM, as of July 26, 2011, there were 11,268 Linux/Unix NIPRNet computer systems within DoD.[2] Also, according to the FY 2010 FISMA report, 34 out of 36 DoD Components reported that they used non-Windows operating systems.

---

[1] The Open Group, who held the Unix trademark, registered various operating systems using the single Unix specification, which included Macintosh, Solaris, Hewlett Packard Unix, and Advanced Interactive eXecutive.

[2] According to USCYBERCOM, the total number of Linux/Unix computer systems within DoD did not include Army systems. Therefore, the number of Linux/Unix computer systems should be higher.

Table 1 shows the number and percentage of DoD Components that use the most common non-Windows operating systems within DoD.

~~(FOUO)~~ Table 1. Non-Windows Operating Systems Used by DoD Components

Operating System	Number of DoD Components	Percentage of DoD Components
Linux	30	83.3 percent
Solaris	28	77.8 percent
Sun	16	44.4 percent
Macintosh Operating System X version 10.6	12	33.3 percent
Hewlett Packard Unix	9	25.0 percent
Advanced Interactive eXecutive	8	22.2 percent
Macintosh Operating System X version 10.5	8	22.2 percent
Berkeley Software Distribution	7	19.4 percent

Installation of HIDS on Non-Windows Computer Systems

~~(FOUO)~~ According to data received from USCYBERCOM and generated by HBSS as of July 26, 2011, DoD Components installed HIPS on 2,120 non-Windows NIPRNet computer systems (all had Linux/Unix operating systems). Therefore, based on the 11,268 Linux/Unix NIPRNet computer systems that USCYBERCOM identified, 9,148 Linux/Unix NIPRNet computer systems did not have HIPS installed. USCYBERCOM and DISA personnel did not know of other HIDS being used within DoD besides HIPS.

> *~~(FOUO)~~ 9,148 Linux/Unix NIPRNet computer systems did not have HIPS installed.*

~~(FOUO)~~ Personnel at FHP&R and at DMEA did not install HIDS on non-Windows NIPRNet computer systems. Personnel at FHP&R, which reports to the Assistant Secretary of Defense (Health Affairs), identified nine non-Windows NIPRNet computer systems, and we verified that all nine non-Windows systems did not have HIDS installed. Personnel at DMEA, which reports to the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, identified one non-Windows NIPRNet system, and we verified that the one non-Windows computer system did not have HIDS installed. We did not review non-Windows SIPRNet systems at FHP&R and DMEA.

~~(FOUO)~~ Sensitive Data on Non-Windows Systems Without HIDS

~~(FOUO)~~ We identified non-Windows computer systems at a DISA location that contained sensitive data and, according to HBSS data, did not have HIPS installed. According to DISA, six non-Windows computer systems, three of which were servers, contained medical records. Medical records should be protected from disclosure under the Health Insurance Portability and Accountability Act. Medical records often include personally identifiable information, such as names, social security numbers, and dates of

birth, as well as patient history, including treatments and health conditions that are very personal in nature. Also, DoD computer systems can contain other sensitive data, such as personnel and financial records.

~~(FOUO)~~ No Requirement for HIDS on Non-Windows Computer Systems

~~(FOUO)~~ USCYBERCOM did not require DoD Components to install HIDS on computer systems with operating systems other than Windows. USCYBERCOM appropriately decided to focus efforts on Windows computer systems first because of inherent vulnerabilities and approximately 99 percent of DoD computer systems had Windows operating systems.

~~(FOUO)~~ FRAGO 13 only requires DoD Components to install the HBSS HIPS component to workstations and servers on supported Windows operating systems with the future capability of installing HIPS on other operating systems. Therefore, DoD Components were not required to install HIDS on computer systems with non-Windows operating systems, such as Linux. However, FRAGO 13 required DoD Components to install the McAfee Agent on LINUX and UNIX computer systems by December 2010 and prepare for the installation of other HBSS products.

~~(FOUO)~~ Although DoD Components are not required to install HIDS on non-Windows computer systems, we identified 10 DoD Components that installed HIPS on at least 1 computer system with a non-Windows operating system. Also, DISA provides the HIPS software on the DoD Patch Repository for certain non-Windows operating systems. Therefore, although USCYBERCOM only requires HIPS installation on supported Windows computer systems, other operating systems were compatible with the HIPS software. Table 2 shows the non-Windows operating systems that were compatible with HIPS software.

Table 2. HIPS Compatibility for Non-Windows Operating Systems

Operating System	HIPS Compatibility
Red Hat Enterprise Linux 5.x	Yes
Red Hat Enterprise Linux 4.x	Yes
Solaris 10	Yes
Solaris 9 (SPARC)	Yes
Solaris 8 (SPARC)	Yes
SuSE Novell Open Enterprise Server (Linux) 10	Yes

~~(FOUO)~~ USCYBERCOM did not develop a formal plan to implement HIDS on computer systems with non-Windows operating systems. FRAGO 13 requires DoD Components to take initial steps for the installation of HBSS products, including HIPS on Linux and Unix operating systems; however, additional guidance was not provided. According to DISA personnel, other controls, such as Security-Enhanced Linux, could be installed on computer systems to provide comparable security to HIPS. USCYBERCOM should develop a formal plan, including milestones to deploy HIDS or other comparable security measures to non-Windows computer systems. At the time of the audit, HIDS deployment was not possible on some operating systems unless the software is modified or new software is developed. The plan should take into account the feasibility of installing HIPS on operating systems that are currently not compatible.

~~(FOUO)~~ FRAGO 13 requires DoD Components to take initial steps for the installation of HBSS products, including HIPS on Linux and Unix operating systems; however, additional guidance was not provided.

Increased Risk to DoD Systems and Sensitive Data

~~(FOUO)~~ DoD requires its Components to use other controls, such as network firewalls and network intrusion detection systems that may detect and prevent unauthorized activity, such as unauthorized access to personal medical information. However, HIDS detects activity that may bypass these controls. In addition, if an unauthorized individual gains access to one system, the individual may be able to gain access to other systems on the same network. We identified nine non-Windows computer systems at FHP&R and one computer system at DMEA that did not have HIDS installed. DoD computer systems that do not have HIDS or other comparable security measures installed might allow intrusions to go undetected. As a result, 9,148 DoD non-Windows systems (including those containing medical records) may be at an increased risk of unauthorized activity, such as critical system file modifications and unauthorized access. Additionally, attacks may go unreported and unmitigated and DoD could incur costs associated with attacks.

Recommendation, Management Comments, and Our Response

~~(FOUO)~~ A. We recommend the Commander, U.S. Cyber Command, develop a formal plan, including milestones, to deploy host-based intrusion detection systems or other comparable security measures to non-Windows computer systems where feasible.

U.S. Cyber Command Comments

~~(FOUO)~~ The Commander, USCYBERCOM, agreed. He stated USCYBERCOM appropriately focused on the security of Windows systems, which represented 99.5 percent of DoD systems and are more vulnerable to attack. The Commander, USCYBERCOM, estimated that 58 percent of known DoD non-Windows systems were compatible with HIPS. Of the 58 percent, 19 percent currently have HIPS installed and 39 percent do not have HIPS installed. He stated that USCYBERCOM will issue a task order requiring HIPS on all remaining compatible systems by March 31, 2012.

~~(FOUO)~~ The Commander stated that 12 percent of known DoD non-Windows systems are not compatible with HIPS. He stated that USCYBERCOM will submit requirements to DISA by December 31, 2011, to develop HIPS versions for operating systems that are currently not compatible with HIPS.

~~(FOUO)~~ Finally, the Commander stated that data is not available on the type of operating systems being used for 30 percent of known DoD non-Windows systems. He further stated that USCYBERCOM will issue a task order to install the McAfee Agent to all DoD non-Windows systems. Installation of the McAfee Agent will provide USCYBERCOM with information on the operating systems used by these computer systems. However, the Commander stated that there is one known non-Windows system that is not compatible with the McAfee Agent. He stated USCYBERCOM will submit requirements to DISA to correct this, where feasible.

Our Response

The USCYBERCOM comments were responsive, and no additional comments are required.

Finding B. HIPS Not Adequately Configured for Windows NIPRNet Computer Systems

~~(FOUO)~~ According to data provided by USCYBERCOM, DoD Components generally installed HIPS on unclassified, Windows computer systems. However, DoD Components did not configure HIPS in accordance with DoD requirements on 60 percent of DoD's 2.1 million Windows unclassified computer systems. Specifically, at FHP&R and DMEA, we identified only 28 Windows NIPRNet computer systems that did not have HIPS installed out of 548 Windows NIPRNet computer systems at those sites. However, FHP&R and DMEA personnel did not adequately configure HIPS to block potentially harmful applications, and, at FHP&R, personnel did not appropriately configure HIPS to block required HIPS signatures that describe security threats, attack methodologies, and network intrusions. DoD Components did not adequately configure HIPS because:

- personnel believed that the appropriate configuration of HIPS required a large effort, but resources were limited;
- ~~(FOUO)~~ personnel at FHP&R did not realize that HIPS configuration settings were not enabled;
- ~~(FOUO)~~ personnel at FHP&R and DMEA did not fully understand DoD requirements; and
- ~~(FOUO)~~ USCYBERCOM did not have a reliable method to ensure that DoD Components appropriately configured HIPS.

~~(FOUO)~~ As a result, DoD unclassified computer systems may not detect or prevent host-based intrusions, and there is an increased risk to unauthorized activity, such as unauthorized access to personnel and financial records.

HIPS Installed on Most Windows NIPRNet Computer Systems but Configuration Needs Improvement

~~(FOUO)~~ According to data provided by USCYBERCOM, DoD Components generally installed HIPS on Windows NIPRNet computer systems. However, DoD Components did not appropriately configure HIPS to block signatures on 60 percent of DoD's 2.1 million Windows NIPRNet computer systems. Also, at one site that we visited, personnel did not appropriately configure HIPS to block required HIPS signatures.

HIPS Installed on Most Windows NIPRNet Computer Systems

~~(FOUO)~~ According to data provided by USCYBERCOM, as of June 30, 2011, 1.9 million of DoD's 2.1 million Windows NIPRNet computer systems had HIPS installed. USCYBERCOM monitors those DoD Components that have not installed HIPS on all Windows computer systems and works with them to meet the DoD requirements. FRAGO 13 requires all DoD Components to install HIPS software on all NIPRNet computer systems that have supported Windows operating systems. According to DISA personnel and the unclassified HBSS Web site, HIPS was compatible with all

current Windows Server operating systems[3] and most current Windows client operating systems.[4]

~~(FOUO)~~ During our limited review at FHP&R and DMEA, we identified only 28 Windows NIPRNet computer systems that did not have HIPS installed out of 548 Windows NIPRNet computer systems at those sites. Specifically at DMEA, we identified 20 Windows NIPRNet computer systems that did not have HIPS installed out of 116 Windows NIPRNet computer systems. We statistically selected and reviewed 22 of 83 computer systems that DMEA reported as having HIPS installed and we confirmed through our review that all 22 had HIPS installed. Additionally, we reviewed 30 of the 33 computer systems that DMEA reported as not having HIPS installed and found that only 20 did not have HIPS installed. According to DMEA personnel, the 20 systems did not have HIPS installed because it could interfere with critical personnel safety systems and because the vendors for some computer systems would not allow the addition of other applications, such as HIPS, on their proprietary Windows systems.

~~(FOUO)~~ At FHP&R, we identified 8 Windows NIPRNet computer systems that did not have HIPS installed out of 432 Windows NIPRNet computer systems. We statistically selected and reviewed 31 of 307 computer systems that FHP&R reported as having HIPS installed and we confirmed through our review that all 31 had HIPS installed. Additionally, we reviewed 49 of the 125 computer systems that FHP&R reported as not having HIPS installed and found that only 8 did not have HIPS installed. The FHP&R HBSS administrator stated that he was not informed that one of the computer systems was added to the inventory and he did not know why the other seven did not have HIPS installed.

Inadequate Configuration of HIPS at Some DoD Components

Some DoD Components did not appropriately configure HIPS to adequately block unauthorized activity. Additionally, some DoD Components did not appropriately configure HIPS to enable application blocking.

Inadequate Configuration of HIPS to Block Unauthorized Activity

~~(FOUO)~~ According to USCYBERCOM and based on self-reported data, as of June 30, 2011, DoD Components did not adequately configure HIPS on 60 percent of DoD Windows NIPRNet computer systems to block high, medium, and low-severity HIPS signatures, as required by FRAGO 13. As of February 28, 2010, FRAGO 13 required DoD Components to block high and medium-severity HIPS signatures while logging low-severity signatures on Windows servers. As of June 30, 2010, FRAGO 13 required DoD Components to block all high, medium, and low-severity HIPS signatures on

[3] Current Windows server operating systems included Windows 2000, Windows 2000 Advanced, Windows 2003 (32-bit and 64-bit), Windows 2003 R2 (32-bit and 64-bit), and Windows 2008 (32-bit and 64-bit) and 2008 R2.

[4] Current Windows workstation operating systems included Windows 2000, Windows XP (32-bit), Windows Vista (32-bit and 64-bit) and Windows 7 (32-bit and 64-bit). Software was not compatible with Windows XP (64-bit).

Windows workstations. According to the USCYBERCOM data, DoD Components adequately configured HIPS on 90 percent of DoD Windows NIPRNet computer systems to block high-severity signatures.

~~(FOUO)~~ FHP&R personnel did not properly configure HIPS to block the appropriate HIPS signatures. During our site visit to FHP&R, we determined that personnel configured HIPS settings to prevent high-severity signatures for workstations and servers, but did not enable those settings for any of the systems. Therefore, HIPS did not provide protection to any of the NIPRNet workstations and servers. Even if HIPS protection was enabled, FHP&R personnel did not configure the settings to prevent medium-severity signatures against NIPRNet servers and personnel did not configure the settings to prevent medium and low-severity signatures against NIPRNet workstations, as required by FRAGO 13. Although we found that FHP&R was not properly blocking signatures, the self-reported data that we obtained from USCYBERCOM showed that the TRICARE Management Activity, under which FHP&R was grouped, reported that it complied with blocking signatures.

~~(FOUO)~~ Even if HIPS protection was enabled, FHP&R personnel did not configure the settings to prevent medium-severity signatures against NIPRNet servers...

Inadequate Configuration of HIPS to Enable Application Blocking

~~(FOUO)~~ DMEA and FHP&R personnel did not configure HIPS to enable application blocking, as required by FRAGO 13. FHP&R personnel did not enable application blocking for its NIPRNet servers. Further, FHP&R personnel did not configure six items that were required to be blocked through application blocking on FHP&R workstations and servers, as required by USCYBERCOM Communications Tasking Order 10-015B, "Directive to Counter Intrusion Activity," June 30, 2010. FRAGO 13 Tab 6 requires DoD Components to enforce application blocking on computers with the Windows server operating system. According to DISA documents, an administrator can use application blocking to specify which applications it will or will not allow to run. An administrator can also use application blocking to allow or disallow applications to link to other applications. For example, a malicious application may attempt to use Microsoft Outlook to send malicious e-mails. Personnel could use application blocking to prevent this action.

~~(FOUO)~~ DMEA personnel enabled application blocking for DMEA servers; however, they did not properly configure application blocking. Instead of creating the allowed and blocked programs within the application blocking module, DMEA personnel created more than 500 trusted applications. According to DISA documentation, personnel should only create trusted applications for limited situations. McAfee documentation stated that trusted applications are application processes that ignore intrusion prevention system, firewall, or application blocking rules. For example, if an application such as a database application is established as a trusted application, most processes that it might run will be allowed. DISA personnel stated there should only be approximately 10 trusted applications, which are primarily associated with McAfee and HBSS software.

(~~FOUO~~) DMEA personnel also did not properly configure the six items that were required to be blocked through application blocking on DMEA workstations as required by Communications Tasking Order 10-015B. DMEA personnel added the items to the workstation settings; however, application blocking was in adaptive mode for workstations, where rules are learned automatically. According to McAfee, when application blocking is in adaptive mode, unauthorized activity is not blocked.

> *(~~FOUO~~) DMEA personnel added the items to the workstation settings; however, application blocking was in adaptive mode for workstations... According to McAfee, when application blocking is in adaptive mode, unauthorized activity is not blocked.*

Reasons for Inadequate Configuration of HIPS

DoD Components did not adequately configure HIPS because:

- DoD Components believed that the appropriate configuration of HIPS required a large effort, but resources were limited;
- (~~FOUO~~) personnel at one DoD Component that we visited did not realize HIPS configuration settings were not enabled;
- (~~FOUO~~) personnel at two DoD Components that we visited did not fully understand DoD requirements; and
- (~~FOUO~~) USCYBERCOM did not have a reliable method to ensure that DoD Components appropriately configured HIPS.

Limited Resources and Large Effort to Configure HIPS

Resources, such as costs to install and configure HBSS, were limited for DoD Components to meet HBSS requirements. In addition, DoD Components believed that the appropriate configuration of HIPS required a large effort.

Limited Resources for DoD Components

(~~FOUO~~) DISA entered into a contract to purchase a license for HIPS to be installed on up to 5 million desktops. However, DoD Components incurred most of the costs to install, configure, and monitor HBSS. These costs included salaries of HBSS administrators and analysts, the acquisition of computer equipment that ran the NIPRNet HBSS server, as well as other direct and indirect costs. For example, according to personnel from the U.S. Fleet Cyber Command/U.S. Tenth Fleet, the Navy estimated that it would cost $33.7 million by the end of FY 2011 to deploy HBSS components to approximately 350 U.S. Naval vessels that have SIPRNet capabilities.

DISA provided some resources to DoD Components to implement HBSS requirements. The HBSS contract provides virtual on-demand training and classroom training to those personnel with HBSS responsibilities. The contract also provided access to technical support as well as deployment and implementation support to DoD Components relating to equipment installation, site configuration, system administration, and monitoring support of HBSS. The DISA Implementation Support Team also provides assistance to

DoD Components that have difficulty in deploying HBSS, including the configuration of HIPS.

Large Effort Required to Configure HIPS

(~~FOUO~~) We identified five DoD Components that experienced problems with being able to appropriately configure HIPS because of the large amount of effort involved. DISA personnel also believed that properly configuring HIPS required a large effort. According to a USCYBERCOM document, which summarizes Plans of Action & Milestones documents submitted by DoD Components, three DoD Components requested extensions to meet configuration requirements because of funding constraints and loss of or lack of qualified HBSS personnel.

(~~FOUO~~) According to personnel from the DISA Implementation Support Team, some DoD Components believed that configuring HIPS in accordance with requirements might disrupt operations. Marine Corps Network Operations Security Center personnel stated that the Marine Corps achieved a high rate of compliance for blocking the required signatures. However, the Marine Corps personnel stated that the success came with a lot of hard work. They stated that there were several instances where HIPS software caused services to stop functioning. They also stated that for each of these problems, it took some effort to correct the issue so that the HIPS software would allow the programs to appropriately operate.

(~~FOUO~~) The HBSS administrator for FHP&R stated that enabling application blocking would require a significant amount of time and resources. He said that to adequately implement application blocking, he would need to create unique configurations for each system and would need to coordinate with system administrators, as well as modify existing policy. The HBSS administrator stated that only about 10 percent of his time was devoted to HBSS-related activities and that FHP&R did not have the resources to fully implement application blocking at the time of our visit. While we recognize that deployment and appropriate configuration of HIPS required a large effort, it is essential that DoD Components fully adhere to DoD requirements to overcome a gap in sufficient security measures deployed on computer systems.

Lack of Awareness That HIPS Protection Was Not Enabled

(~~FOUO~~) FHP&R did not block high-severity HIPS signatures because personnel did not realize that the HIPS settings were not enabled. FHP&R personnel configured HIPS to block high-severity signatures, but did not enable or turn on the HIPS protection. FHP&R personnel stated that this occurred because FHP&R recently migrated the NIPRNet HBSS server from an older version to a current version and the personnel did not realize the policy was not enabled since the upgrade.

Lack of Understanding of HIPS Requirements

(~~FOUO~~) FHP&R did not configure HIPS to properly prevent medium-severity HIPS signatures for servers and medium and low-severity HIPS signatures for workstations because the HBSS administrator did not recently review the DoD requirements and, therefore, did not fully understand what protection was required. However, since our

review, FHP&R personnel took appropriate actions to block HIPS signatures in accordance with the DoD requirements.

~~(FOUO)~~ Additionally, FHP&R did not enable Application Blocking for servers and did not configure workstations and servers to block the six required blacklisted items because the HBSS administrator originally thought that application blocking was only required for critical systems. FHP&R should enable HIPS application blocking on Windows NIPRNet servers and configure HIPS application blocking to block the required blacklist items for Windows NIPRNet workstations and servers.

~~(FOUO)~~ DMEA did not appropriately configure Application Blocking on Windows NIPRNet workstations and servers because the HBSS administrator did not know how to correctly create application blocking rules. We referred the HBSS administrator to the specific documents to review. The HBSS administrator took immediate action on the issue for the Windows NIPRNet workstations. However, the HBSS administrator still must correct the application blocking configuration for Windows NIPRNet servers. DMEA should configure application blocking for Windows NIPRNet servers in accordance with DoD guidance.

~~(FOUO)~~ No Reliable Method to Oversee Configuration of HIPS

~~(FOUO)~~ USCYBERCOM did not have a reliable method to ensure that DoD Components appropriately configured HIPS on computer systems within DoD. USCYBERCOM relied on responses from DoD Components to determine whether they configured HIPS in accordance with USCYBERCOM requirements. USCYBERCOM compiled statistics on a weekly basis on each DoD Component's compliance for blocking high, medium, and low-severity HIPS signatures. To determine the blocking status, USCYBERCOM relied on data reported by DoD Components within the Vulnerability Management System. Not only is the data self-reported, it also appeared to be inaccurate because some DoD Components reported their blocking status as 0 percent for each category. Additionally, we identified one organization that was not blocking medium and low-severity signatures; however, the organization they were reported under showed the organization was blocking high, medium, and low-severity signatures for 100 percent of their systems. USCYBERCOM should develop and submit requirements to DISA to develop an automated method to determine whether DoD Components are appropriately configuring HIPS on computer systems and should order DoD Components to report HIPS configuration information through the automated method once the capability exists. Finally, DISA should develop the automated method.

> *(~~FOUO~~) Not only is the data self-reported, it also appeared to be inaccurate because some DoD Components reported their blocking status as 0 percent for each category.*

Increased Risk to Unauthorized Activity

~~(FOUO)~~ As a result of not appropriately configuring HIPS on Windows NIPRNet workstations and servers, DoD computers are at an increased risk to unauthorized activity, such as critical system file modifications and unauthorized access to personnel

or financial data. For example, an individual may modify system files that destroy the reliability of financial records. HIPS, if deployed correctly, can significantly reduce the exposure to certain threats and vulnerabilities. According to the HBSS Quick Reaction Test Final Report, January 3, 2011, tests showed that HIPS protected computer systems from unauthorized activity that would not have otherwise been prevented without HIPS. The HIPS software was customizable, and during tests, personnel added enhancements to HBSS to increase its protection capability. The tests allowed DoD personnel to assess the capabilities provided by HBSS and areas that needed improvement. The HIPS software provides a mechanism to adjust and respond to attacks. Additionally, because USCYBERCOM did not have a reliable method to ensure that DoD Components appropriately configured HIPS on computer systems, USCYBERCOM may not be able to adequately determine whether DoD Components are able to detect and prevent threats as required by DoD guidance and adequately follow up with the Components on why they are not adhering to DoD requirements.

Actions Taken to Reduce Risk

~~(FOUO)~~ During the course of our audit, FHP&R and DMEA personnel took some corrective actions to reduce the risk of unauthorized activity. FHP&R personnel enabled HIPS on its Windows NIPRNet workstations and servers. Further, FHP&R personnel configured HIPS to block high, medium, and low-severity signatures on workstations and to block high and medium-severity signatures on servers. DMEA personnel configured HIPS application blocking to block the six items on DMEA workstations as required by Communications Tasking Order 10-015B.

Conclusion

~~(FOUO)~~ HIPS plays an important role in DoD's computer network defense by providing an additional layer of defense against intrusions. HIPS monitors and blocks intrusions and protects against known and unknown malicious activity. DoD Components did not fully configure HIPS on computer systems as required by DoD requirements. As a result, there is an increased risk to workstations and servers and the sensitive data contained within could be compromised.

Recommendations, Management Comments, and Our Response

B.1. We recommend the Commander, U.S. Cyber Command:

~~(FOUO)~~ a. Develop and submit requirements to the Defense Information Systems Agency to develop an automated method to determine whether DoD Components are appropriately configuring the Host Intrusion Prevention System on computer systems.

U.S. Cyber Command Comments

~~(FOUO)~~ The Commander, USCYBERCOM, agreed with the recommendation and the associated internal control weakness. The Commander stated in his response to the internal control weakness that USCYBERCOM is working on a near-term effort to

require DoD Components to periodically query their HBSS servers and provide the results to USCYBERCOM. The Commander also stated that DISA and McAfee would develop a method for configuration metrics to be automatically sent from DoD Components to USCYBERCOM. He stated that USCYBERCOM will submit requirements to DISA for this automated reporting capability by March 31, 2012. Finally, the Commander stated that USCYBERCOM and DISA would also include these requirements in a request for proposal by September 2012 in planning for a second generation HBSS replacement.

Our Response

The USCYBERCOM comments were responsive, and no additional comments are required.

~~(FOUO)~~ b. Require DoD Components to report Host Intrusion Prevention System configuration information through the automated method, once the capability exists, referred to in recommendations B.1.a and B.2.

U.S. Cyber Command Comments

~~(FOUO)~~ The Commander, USCYBERCOM, agreed with the recommendation and the associated internal control weakness. The Commander indicated USCYBERCOM is preparing a task order requiring DoD Components to submit reports periodically by e-mail from their HBSS servers. He stated that the HBSS server can be configured to export and e-mail the reports automatically to ensure they are not modified. The Commander stated that this methodology will not be fully automated, but will provide USCYBERCOM with more accurate configuration data while DISA works with McAfee on a more robust solution. The Commander stated in his response to the internal control weakness that the reports would be mandated by March 31, 2012. The Commander stated that once the fully automated method becomes available, USCYBERCOM will release another task order directing DoD Components to configure the HBSS servers to report configuration information through the automated method.

Our Response

The USCYBERCOM comments were responsive, and no additional comments are required.

(~~FOUO~~) B.2. We recommend the Director, Defense Information Systems Agency, develop the automated capability for U.S. Cyber Command to determine whether DoD Components are appropriately configuring the Host Intrusion Prevention System.

Defense Information Systems Agency Comments

~~(FOUO)~~ The DISA Director for Mission Assurance and Network Operations agreed. The Director stated that DISA delivered the capability for sites to determine their HIPS status and export and e-mail the resulting reports to USCYBERCOM. He stated that efforts were ongoing to automate configuration and site status information, including HIPS

configuration status. The Director stated this fully automated capability will be available by September 30, 2014.

Our Response

The DISA comments were responsive, and no additional comments are required.

B.3. We recommend that the Director, Force Health Protection and Readiness:

(~~FOUO~~) a. Enable Host Intrusion Prevention System application blocking on Windows Unclassified but Sensitive Internet Protocol Router Network servers.

Assistant Secretary of Defense (Health Affairs) Comments

(~~FOUO~~) The Assistant Secretary of Defense (Health Affairs), responding for the Director, Force Health Protection and Readiness, agreed. The Assistant Secretary of Defense (Health Affairs) stated that FHP&R worked with DISA to enable and fully implement HIPS application blocking across all Window NIPRNet servers. He indicated that all actions for this recommendation are complete.

Our Response

The Assistant Secretary of Defense (Health Affairs) comments were responsive, and no additional comments are required.

(~~FOUO~~) b. Configure Host Intrusion Prevention System application blocking to block the required blacklist items for Windows Unclassified but Sensitive Internet Protocol Router Network workstations and servers.

Assistant Secretary of Defense (Health Affairs) Comments

(~~FOUO~~) The Assistant Secretary of Defense (Health Affairs), responding for the Director, Force Health Protection and Readiness, agreed. The Assistant Secretary of Defense (Health Affairs) stated that FHP&R configured HIPS to block the required blacklist items on all FHP&R Windows NIPRNet workstations and servers. He indicated that all actions for this recommendation are complete.

Our Response

The Assistant Secretary of Defense (Health Affairs) comments were responsive, and no additional comments are required.

(~~FOUO~~) B.4. We recommend the Director, Defense Microelectronics Activity, configure application blocking for Windows Unclassified but Sensitive Internet Protocol Router Network servers in accordance with DoD guidance.

Defense Microelectronics Activity Comments

(~~FOUO~~) The Deputy Director, DMEA, agreed. The Deputy Director stated DMEA was implementing corrective actions to ensure compliance with stated DoD requirements. Specifically, he stated DMEA correlated its current list of trusted applications to DISA's

recommended application blocking methodology. The Deputy Director stated that DMEA also developed and tested its HIPS application blocking rule set. He stated that DMEA deployed the application blocking rule set to 8 of 34 Windows NIPRNet servers and will complete the deployment by January 20, 2012.

Our Response

The DMEA comments were responsive, and no additional comments are required.

~~(FOUO)~~ Finding C. Updating HIPS Signatures Can Better Address Threats to DoD

~~(FOUO)~~ HIPS signatures (which describe security threats, attack methodologies, and network intrusions) may not have fully addressed DoD-specific threats. This occurred because USCYBERCOM had not reviewed the list of signatures since 2009 to determine whether the signatures addressed vulnerabilities in DoD. USCYBERCOM relied on HIPS signatures that were developed by McAfee for the commercially-available HIPS product. Additionally, USCYBERCOM focused on other priorities, such as deploying HBSS, and ensuring HBSS was properly configured across DoD. As a result, DoD computer systems may be vulnerable to threats that were developed since the original list of signatures was reviewed and approved in 2009.

Effectiveness of HIPS Signatures to DoD Threats

~~(FOUO)~~ HIPS signatures may not have fully addressed DoD-specific threats. DISA identified 31 HIPS signatures that would provide expanded capabilities to HIPS. According to the HBSS Quick Reaction Test Final Report issued on January 3, 2011, DISA and other organizations conducted a quick reaction test to identify enhancements to HBSS. They developed scenarios and events that tested the capability of HBSS and increased the capabilities of HBSS to address additional needs outlined in the CNCI. During the testing, a threat team launched aggressive threats allowing defenders to identify methods to counter the threats and develop ways to increase capabilities within DoD. While the report found HBSS had the ability to provide significant protection and detection capabilities, HBSS was unable to protect systems from many of the advanced attack techniques used by the opposing threat team. The report revealed a number of technical and procedural improvements that can be implemented to defend against many of the threats. Also, DISA reported that improvements made in the testing environment raised the overall capability level of HBSS. In fact, the report showed that enhancements provided additional protection in 7 of 12 scenarios. As a result of the testing, DISA developed "Host IPS [HIPS] Signatures for Added Detection and Prevention," December 3, 2010, which identified 31 HIPS signatures for added detection and prevention. The DISA document reported that the signatures were successful at providing detection capabilities against various attack vectors. These signatures were not added to the DoD set of HIPS signatures.

~~(FOUO)~~ While the report found HBSS had the ability to provide significant protection and detection capabilities, HBSS was unable to protect systems from many of the advanced attack techniques used by the opposing threat team.

~~(FOUO)~~ Lack of Review of HIPS Signatures

(~~FOUO~~) USCYBERCOM did not review the list of signatures used within HIPS since 2009. According to USCYBERCOM personnel, the JTF-GNO identified a list of more than 700 HIPS signatures in 2009. However, since then, USCYBERCOM relied on HIPS signatures that McAfee developed for the commercially-available HIPS product. These

McAfee signatures were regularly released to the DoD repository for DoD Components to download and use. USCYBERCOM's focus, during this time, was to ensure that HBSS, including HIPS, was properly deployed and to ensure proper configuration of HBSS across DoD. USCYBERCOM should review and update the list of HIPS signatures at least annually to ensure the signatures adequately protect DoD computer systems. USCYBERCOM should take into account threats and vulnerabilities that are unique to DoD that would not otherwise be addressed by the commercially available HIPS software.

Increased Risk to Unauthorized Activity

~~(FOUO)~~ As a result of not reviewing HIPS signatures, DoD computer systems are at an increased risk to unauthorized activity. DoD computer systems might be vulnerable to threats that have been developed since the original list of signatures was reviewed and approved in 2009. Specifically, without the additional signatures recommended by DISA in their Quick Reaction Test report, DoD computer systems could be at risk of similar attacks as demonstrated in their report.

Recommendation, Management Comments, and Our Response

~~(FOUO)~~ C. We recommend that the Commander, U.S. Cyber Command, review and update the list of Host Intrusion Prevention System signatures at least annually to ensure the signatures adequately protect DoD computer systems.

U.S. Cyber Command Comments

~~(FOUO)~~ The Commander, USCYBERCOM, agreed. The Commander stated USCYBERCOM will provide McAfee with areas of concern and McAfee will provide HIPS signatures from their inventory to address those concerns. He stated that DISA will provide testing support to assess the signatures effectiveness and adjust signatures for fielding. The Commander stated that USCYBERCOM will then issue a task order to all DoD Components to ensure compliance. The Commander stated that this process will be mandated by March 31, 2012, and will occur monthly.

Our Response

The USCYBERCOM comments were responsive, and no additional comments are required.

~~(FOUO)~~ Finding D. Creating Access to HBSS NIPRNet Event Data

~~(FOUO)~~ USCYBERCOM could not access NIPRNet HBSS event data. This occurred because DoD encountered capacity complications when consolidating NIPRNet HBSS event data from approximately 2.1 million Windows NIPRNet computer systems. Also, DoD focused first on obtaining SIPRNet HBSS event data because of the sensitivity of the data. As a result, USCYBERCOM may not fully identify cyber trends across DoD.

HBSS Event Data Background

HBSS event data includes specific information on attempted or successful intrusions to computer systems with HIPS installed. It also includes event data from other HBSS components to include the Device Control Module, which can block flash media drives on computer systems. The HBSS event data include dates of occurrence, host name, threat source internet protocol address, threat target internet protocol address, action taken and other information necessary to understand the intrusion. The HBSS event data can help USCYBERCOM monitor DoD networks and identify trends across DoD Components.

> *The HBSS event data can help USCYBERCOM monitor DoD networks and identify trends across DoD Components.*

~~(FOUO)~~ Lack of USCYBERCOM Visibility Over NIPRNet HBSS Event Data

~~(FOUO)~~ USCYBERCOM could not access and review automated NIPRNet HBSS event data because the capability did not exist. However, according to USCYBERCOM personnel, both NIPRNet and SIPRNet HBSS event data were available to DoD component local administrators and network defense personnel for their own analysis. We verified the availability of the HBSS event data at the two sites that we visited.

~~(FOUO)~~ Although NIPRNet HBSS event data were not available, USCYBERCOM could access SIPRNet HBSS event data. We observed SIPRNet HBSS event data at USCYBERCOM and found that SIPRNet HBSS event data were available. We also determined that SIPRNet event data were adequately being reported to USCYBERCOM from two sites that we visited. We obtained 20 logged SIPRNet HBSS events from two sites to determine if the event data were reported and available to USCYBERCOM for their use and determined that all of the event data for the 20 events were available.

~~(FOUO)~~ Complications With Reporting NIPRNet HBSS Event Data and Initial Focus on SIPRNet HBSS Event Data

~~(FOUO)~~ DoD encountered complications with reporting the large amount of NIPRNet HBSS event data. The majority of DoD computer systems, approximately 2.1 million Windows systems alone, were connected to the NIPRNet. As a result, most HBSS event data were generated from NIPRNet computer systems. For example, the Navy had

approximately 1.7 million Navy HBSS events occur on the NIPRNet during the 30-day period before April 29, 2011. We also found that for June 2011, approximately 38.6 million HIPS and malware events occurred on the DoD SIPRNet. USCYBERCOM personnel estimated that they expected the number of DoD NIPRNet HBSS events to be about 10 times the amount of the SIPRNet HBSS events for all of DoD. The volume of NIPRNet systems and HBSS events will also require additional personnel resources to analyze and monitor the event data.

~~(FOUO)~~ Additionally, DoD focused on obtaining SIPRNet HBSS event data first because of the sensitivity of the data. USCYBERCOM decided to ensure that they received the HBSS event data for the classified systems before the unclassified systems to reduce the risk of classified data being compromised. We agree that focusing on obtaining SIPRNet HBSS event data first was appropriate.

Reduced Ability to Identify Threats

~~(FOUO)~~ Without the capability in place to report NIPRNet HBSS event data, USCYBERCOM may not fully identify threats and trends on intrusions across DoD Components affecting the DoD networks and hosts. For example, USCYBERCOM personnel stated that HBSS can detect potential cross-domain violations, which would indicate the possibility that data traversed from the SIPRNet to the NIPRNet. Without the capability to access NIPRNet HBSS event data, USCYBERCOM may not be able to detect those violations.

~~(FOUO)~~ Initial Capability Developed to Consolidate NIPRNet HBSS Event Data

~~(FOUO)~~ According to DISA personnel, DISA developed the initial capability for USCYBERCOM to access NIPRNet HBSS event data and it was technically capable to receive NIPRNet HBSS event data from DoD Components. In fact, DISA personnel indicated that DISA was rolling up their own HBSS event data. However, DISA personnel indicated they were still verifying event volumes at other DoD Components, configuring the capability to handle surges, and determining which events to collect. DISA should fully develop the capability to consolidate NIPRNet HBSS event data to allow USCYBERCOM access to that data. USCYBERCOM should order DoD Components to roll up NIPRNet HBSS event data once the capability exists to fully consolidate that data.

Recommendations, Management Comments, and Our Response

~~(FOUO)~~ D.1. We recommend the Director, Defense Information Systems Agency, fully develop the capability to consolidate Unclassified but Sensitive Internet Protocol Router Network Host Based Security System event data to allow U.S. Cyber Command access to that data.

Defense Information Systems Agency Comments

~~(FOUO)~~ The DISA Director for Mission Assurance and Network Operations agreed. The Director stated that DISA developed an initial capability for reporting unclassified event data. However, he stated that the capability will need an increase in capacity once DoD issues the order for sites to begin reporting their NIPRNet alerts. He stated that DISA will work with USCYBERCOM to ensure the solution meets the operational intent.

Our Response

The DISA comments were responsive, and no additional comments are required.

~~(FOUO)~~ D.2. We recommend the Commander, U.S. Cyber Command, require DoD Components to roll up Unclassified but Sensitive Internet Protocol Router Network Host Based Security System event data once the capability exists to fully consolidate that data.

U.S. Cyber Command Comments

~~(FOUO)~~ The Commander, USCYBERCOM, agreed with the recommendation and the associated internal control weakness. The Commander indicated DISA and DoD Components will require configuration changes and supporting system acquisitions to collect HIPS data from NIPRNet hosts. He stated that because of the volume of data anticipated from the NIPRNet hosts, DoD Components specifically would need intermediate roll-up servers and would need configuration changes to reduce the amount of data flowing to USCYBERCOM. Additionally, he stated that Computer Network Defense Service Providers and DoD Components will have to reconcile reporting responsibilities.

~~(FOUO)~~ The Commander stated USCYBERCOM and DISA will jointly release a data call by March 31, 2012, to determine additional resources Computer Network Defense Service Providers will require to support full NIPRNet reporting. In addition, USCYBERCOM will use the data call to determine implementation timelines.

~~(FOUO)~~ The Commander indicated once HBSS capabilities of the Computer Network Defense Service Providers are assessed, USCYBERCOM will begin limited data collection of the critical incidents first to implement automated reporting thresholds. As the fidelity of the data increases, he stated USCYBERCOM would expand their scope in phases.

Our Response

The USCYBERCOM comments were responsive, and no additional comments are required.

Appendix. Scope and Methodology

We conducted this performance audit from January 2011 through November 2011 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

We met with personnel from the Office of the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer, the Office of the Assistant Secretary of Defense (Health Affairs) FHP&R, USCYBERCOM, DISA, the U.S. Navy, the U.S. Marine Corps, and DMEA.

We reviewed DoD Directive O-8530.1, "Computer Network Defense (CND)," January 8, 2001; Chairman of the Joint Chiefs of Staff Manual 6510.01A, "Information Assurance (IA) and Computer Network Defense (CND) Volume 1 (Incident Handling Program)," June 24, 2009; FRAGO 13; and other orders issued by JTF-GNO and USCYBERCOM. We also reviewed HBSS implementation guidance issued by DISA.

We obtained data from the FY 2010 FISMA report to determine the number of DoD Components that used computer systems with non-Windows operating systems. We also obtained total numbers of DoD Windows NIPRNet computer systems as of June 30, 2011, and DoD Linux/Unix NIPRNet computer systems as of July 26, 2011. The number of DoD computer systems with other operating systems was not available. We obtained HBSS rollup data from USCYBERCOM that captured the deployment of HIPS for Windows NIPRNet computer systems as of June 30, 2011, and for non-Windows NIPRNet computer systems as of July 26, 2011. We also obtained a document from USCYBERCOM that showed the percentage of Windows NIPRNet computer systems blocking high, medium, and low-severity signatures. The percentage was based on DoD Component self-reported data and was as of June 30, 2011. We reviewed the deployment of HIPS at FHP&R and DMEA on NIPRNet systems. Also at those two locations, we reviewed HBSS settings in place to block threats for NIPRNet systems. We also obtained HBSS events from SIPRNet computer systems at those two locations and traced them to a rollup database at USCYBERCOM.

Use of Computer-Processed Data

~~(FOUO)~~ We obtained data from USCYBERCOM that identified numbers of DoD NIPRNet computer systems with Windows operating systems and with non-Windows operating systems (all non-Windows computer systems reported had Linux/Unix operating systems) that had HIPS installed. USCYBERCOM personnel stated they obtained this data from automated rollup information from HBSS. We also obtained data from USCYBERCOM that identified total numbers of DoD NIPRNet computer systems with Windows operating systems and with Linux/Unix operating systems. USCYBERCOM could not identify the total number of DoD NIPRNet computer systems with operating systems other than Windows and Linux/Unix. According to

USCYBERCOM, the total numbers of DoD Windows and Linux/Unix computer systems were self-reported by DoD Components through the Vulnerability Management System and may not be completely accurate. However, we used this data because it was the best data available to provide DoD-level results.

We did not perform tests on this data across DoD because of the time and effort that would have been needed to perform those tests. However, we performed tests on computer systems at FHP&R and DMEA where HBSS reported that HIPS was installed. We reviewed statistical samples of 53 computer systems at the 2 locations that we visited that were reported by HBSS to have HIPS installed; 31 computer systems at FHP&R and 22 computer systems at DMEA. Of the 53 computer systems reviewed, we determined that all 53 were correctly reported as having HIPS installed.

Use of Technical Assistance

DoD Office of Inspector General Information Systems Directorate aided the team in reviewing the HBSS settings at the two sites that we visited. They also participated in discussions at USCYBERCOM and DISA.

DoD OIG Quantitative Methods and Analysis Division also assisted the team in performing the audit and provided assistance in generating statistical samples of computer systems to review at FHP&R and DMEA. We did not project the results of the statistical samples because the team did not identify any computer systems in the samples that were misreported.

Prior Coverage

No prior coverage has been conducted on HIDS within DoD during the last 5 years.

Glossary

Application blocking – Allows the use of a limited subset of required and approved applications and all others are blocked.

Host Based Security System (HBSS) – Commercial off-the-shelf application that monitors, detects, and counters against known cyber threats to the DoD enterprise.

Host Based Security System (HBSS) event data – This data includes specific information on attempted or successful intrusions into computer systems with HIPS installed. Specifically, it includes dates of occurrence, host name, threat source internet protocol address, threat target internet protocol address, action taken and other information necessary to understand the intrusion.

Host Intrusion Prevention System (HIPS) – A component in HBSS that monitors and blocks intrusions and protects against known and unknown malicious activity, including worms, Trojan horses, buffer overflow attacks, malformed commands, critical system file modifications, unauthorized access, and privilege escalation.

Host Intrusion Prevention System (HIPS) Signatures – Used to describe security threats, attack methodologies, and network intrusions.

High-severity signatures – Indicates clearly identifiable security threats or malicious actions, and indicate well-identified vulnerabilities. These signatures include protection from known critical vulnerabilities.

Medium-severity signatures – Identify behavioral activity where applications operate outside of their environment. These signatures include protection for vulnerabilities that exhibit a slightly higher chance for incorrect detection. These signatures become increasingly behavior-based, and are less reliant on a specific attack.

Low-severity signatures – Identify behavioral activity even though applications and system resources are locked and cannot be changed.

Information signatures – Indicate modification to the system configuration but are not generally evidence of an attack.

Intrusion Detection System (IDS) – Software or a physical appliance that monitors traffic in order to detect unwanted traffic that violates acceptable use policies.

Host-based IDS (HIDS) – Must be installed at each machine and analyzes network traffic and system-specific settings such as local security settings.

Network IDS – Installed on the network and analyzes network traffic for suspicious activity in order to make decisions about the traffic.

Wireless IDS – Analyzes wireless-specific traffic, including scanning for external users trying to connect to access points, introduction of rogue access points, and users connecting to the network outside the physical area of the company.

McAfee Agent – The software agent on a host system that provides local management of all HBSS products installed on the host.

Operating systems – Software that resides on computers, which communicates with computer hardware and allows users to utilize programs and applications through a user interface.

Secret Internet Protocol Router Network (SIPRNet) – DoD's largest interoperable command and control data network, supporting the Global Command and Control System, the Defense Message System, collaborative planning and numerous other classified warfighter applications.

Server – A computer in a network that is used to provide services to other computers in the network.

Trusted applications – Applications that are trusted to perform most operations and will ignore all IPS, firewall, and application blocking rules.

Unclassified but Sensitive Internet Protocol Router Network (NIPRNet) – A global network within DoD that that supports unclassified data communications services.

Assistant Secretary of Defense (Health Affairs) Comments

THE ASSISTANT SECRETARY OF DEFENSE
1200 DEFENSE PENTAGON
WASHINGTON, DC 20301-1200

HEALTH AFFAIRS

DEC 13 2011

MEMORANDUM FOR INSPECTOR GENERAL, DEPARTMENT OF DEFENSE
PROGRAM DIRECTOR, READINESS, OPERATIONS, AND SUPPORT

SUBJECT: Department of Defense Response to the Department of Defense Inspector General Draft Report, Project No. D2011-D000LB-0124.000, "Improvements Needed With Host-Based Intrusion Detection Systems"

This is the Department of Defense (DoD) response to DoD Inspector General (IG) draft report, Project No. D2011-D000LB-0124.000, "Improvements Needed With Host-Based Intrusion Detection Systems." Thank you for the opportunity to review the draft report and provide comments. My attached response addresses specific comments on the overall DoD IG's review findings and recommendations. All actions are complete, so we recommend closure of this report. Please direct any comments to the action officers on this topic, (b) (6) (Functional), or (b) (6) (Audit Liaison). (b) (6) may be reached at (b) (6)

(b) (6)

Jonathan Woodson, [redacted]

Attachment:
As stated

DEPARTMENT OF DEFENSE OFFICE OF THE INSPECTOR GENERAL
DRAFT REPORT – DATED NOVEMBER 8, 2011
PROJECT NO. D2011-D000LB-0124.000
"IMPROVEMENTS NEEDED WITH HOST-BASED INTRUSION DETECTION SYSTEMS"
FORCE HEALTH PROTECTION AND READINESS COMMENTS TO THE RECOMMENDATIONS

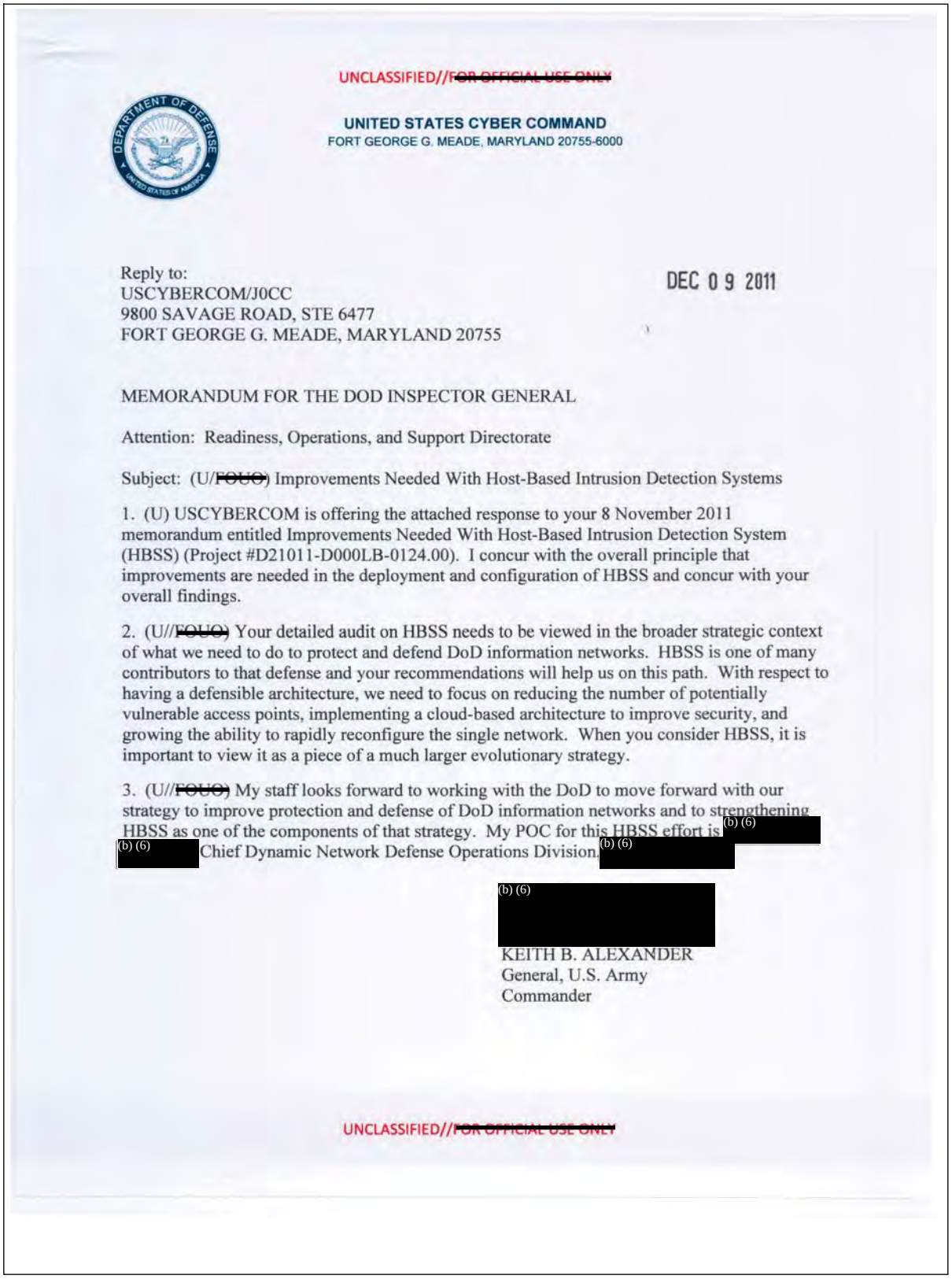
RECOMMENDATION B.3.: We recommend that the Director, Force Health Protection and Readiness:

a. Enable Host Intrusion Prevention System application blocking on Windows Unclassified but Sensitive Internet Protocol Router Network servers.

b. Configure Host Intrusion Prevention System application blocking to block the required blacklist items for Windows Unclassified but Sensitive Internet Protocol Router Network workstations and servers.

FHP&R RESPONSE: Concur. When Force Health Protection and Readiness became aware of these recommendations, work to enable Host Intrusion Prevention System application blocking began immediately. Assisted by Defense Information Systems Agency deployment team members, we enabled and fully implemented application blocking, across all Windows Unclassified but Sensitive Internet Protocol Router Network servers. At the same time, we configured the Host Intrusion Prevention System application to block the required blacklist items on all Force Health Protection and Readiness Windows Unclassified but Sensitive Internet Protocol Router Network workstations and servers. All actions are complete.

U.S. Cyber Command Comments



UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

UNITED STATES CYBER COMMAND
FORT GEORGE G. MEADE, MARYLAND 20755-6000

Reply to:
USCYBERCOM/J0CC
9800 SAVAGE ROAD, STE 6477
FORT GEORGE G. MEADE, MARYLAND 20755

DEC 0 9 2011

MEMORANDUM FOR THE DOD INSPECTOR GENERAL

Attention: Readiness, Operations, and Support Directorate

Subject: (U//~~FOUO~~) Improvements Needed With Host-Based Intrusion Detection Systems

1. (U) USCYBERCOM is offering the attached response to your 8 November 2011 memorandum entitled Improvements Needed With Host-Based Intrusion Detection System (HBSS) (Project #D21011-D000LB-0124.00). I concur with the overall principle that improvements are needed in the deployment and configuration of HBSS and concur with your overall findings.

2. (U//~~FOUO~~) Your detailed audit on HBSS needs to be viewed in the broader strategic context of what we need to do to protect and defend DoD information networks. HBSS is one of many contributors to that defense and your recommendations will help us on this path. With respect to having a defensible architecture, we need to focus on reducing the number of potentially vulnerable access points, implementing a cloud-based architecture to improve security, and growing the ability to rapidly reconfigure the single network. When you consider HBSS, it is important to view it as a piece of a much larger evolutionary strategy.

3. (U//~~FOUO~~) My staff looks forward to working with the DoD to move forward with our strategy to improve protection and defense of DoD information networks and to strengthening HBSS as one of the components of that strategy. My POC for this HBSS effort is (b) (6) (b) (6) Chief Dynamic Network Defense Operations Division, (b) (6)

(b) (6)

KEITH B. ALEXANDER
General, U.S. Army
Commander

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

Recommendations *Project No. D2011-D000LB-0124.000 8 November 2011*

~~(FOUO)~~ **A.** We recommend the Commander, U.S. Cyber Command, develop a formal plan including milestones to deploy host-based intrusion detection systems or other comparable security measures to non-Windows computer systems where feasible.

~~(FOUO)~~ **B.1.** We recommend the Commander, U.S. Cyber Command:

- ~~(FOUO)~~ **a**. Develop and submit requirements to the Defense Information Systems Agency to develop an automated method to determine whether DoD Components are appropriately configuring the Host Intrusion Prevention System on computer systems.

- ~~(FOUO)~~ **b.** Require DoD Components to report Host Intrusion Prevention System configuration information through the automated method, once the capability exists, referred to in recommendations B.1.a and B.2.

~~(FOUO)~~ *B.2. We recommend the Director, Defense Information Systems Agency, develop the automated capability for U.S. Cyber Command to determine whether DoD Components are appropriately configuring the Host Intrusion Prevention System.*

~~(FOUO)~~ *B.3. We recommend that the Director, Force Health Protection and Readiness:*

- ~~(FOUO)~~ *a. Enable Host Intrusion Prevention System application blocking on Windows Unclassified but Sensitive Internet Protocol Router Network servers.*

- ~~(FOUO)~~ *b. Configure Host Intrusion Prevention System application blocking to block the required blacklist items for Windows Unclassified but Sensitive Internet Protocol Router Network workstations and servers.*

~~(FOUO)~~ *B.4. We recommend the Director, Defense Microelectronics Activity, configure application blocking for Windows Unclassified but Sensitive Internet Protocol Router Network servers in accordance with DoD guidance.*

~~(FOUO)~~ **C.** We recommend that the Commander, U.S. Cyber Command, review and update the list of Host Intrusion Prevention System signatures at least annually to ensure the signatures adequately protect DoD computer systems.

~~(FOUO)~~ *D.1. We recommend the Director, Defense Information Systems Agency, fully develop the capability to consolidate Unclassified but Sensitive Internet Protocol Router Network Host Based Security System event data to allow U.S. Cyber Command access to that data.*

~~(FOUO)~~ **D.2.** We recommend the Commander, U.S. Cyber Command, require DoD Components to roll up Unclassified but Sensitive Internet Protocol Router Network Host Based Security System event data once the capability exists to fully consolidate that data.

UNCLASSIFIED/~~FOR OFFICIAL USE ONLY~~

Recommendations ***Project No. D2011-D000LB-0124.000***
8 November 2011

CYBERCOM RECOMMENDATIONS

~~(FOUO)~~ A. We recommend the Commander, U.S. Cyber Command, develop a formal plan including milestones to deploy host-based intrusion detection systems or other comparable security measures to non-Windows computer systems where feasible.

USCYBERCOM agrees with this recommendation.

1. There are only 11.2K known non-Windows systems in the DoD, representing 0.5% of the DoD system inventory. USCYBERCOM appropriately focused security mitigation on the 99.5% majority of systems, those running the Windows operating system and vulnerable to attack both in terms of technical exploits, mission risk, and footprint. The IG Audit recognizes USCYBERCOM's focus within the report.

2. The Host Intrusion Prevention System (HIPS) is one of eight components of McAfee's Host Based Security System (HBSS). HBSS is the tool suite acquired by the Enterprise Solutions Steering Group to perform Defensive Cyber Operations at the local/host level. The HIPS module specifically provides intrusion detection and prevention capability on individual hosts (workstations/laptops/servers) and was therefore among the foci of the DoD IG's audit of DoD Intrusion Detection Systems.

3. During initial fielding in late 2008[1] the HIPS component was only mandated on systems running a Windows operating system. (As previously stated this was done because Windows systems represent 99.5% of the hosts connected to the Enterprise and are subsequently the largest attack surface.)

4. Of the known DoD hosts that run a non-Windows operating system the following is true:

   a. 19% have HIPS installed

   b. 39% are compatible with HIPS, but it is not installed

   c. 12% - HIPS is not compatible and therefore cannot be installed at this time

   d. 30% - No data is available on the operating system being used

5. To meet this recommendation of fielding HIPS to systems running non-Windows operating systems, USCYBERCOM plans to do the following:

---

[1] Reference FRAGO 13 to JTF-GNO OPORD 05-01; HBSS

UNCLASSIFIED/~~FOR OFFICIAL USE ONLY~~

a. Release a TASKORD to all DoD Components mandating the installation and use of HIPS on all compatible systems. This will keep HIPS on the 19% of non-Windows systems where it is already installed and roll-out HIPS on an additional 39%, giving us 58% coverage of non-Windows systems. This TASKORD is due for release during the second quarter of FY12.

b. Develop operational/functional/technical requirements and staff them to DISA for the development of HIPS versions that are compatible with the operating systems used on the currently non-compatible systems. These requirements will be staffed to DISA by end of CY 11. Development efforts will be prioritized by the prevalence of each operating system.

c. The fact that data is not available on 30% of the non-windows system is due to the fact that FRAGO 13 only mandated installation of the data collection and transmission component of HBSS, i.e, the McAfee Agent, on Linux/Unix systems and not all non-Windows systems. This will be rectified in the TASKORD referenced above with the mandate to install the McAfee Agent on all non-Windows systems.

Note: This will still leave a small percentage of non-Windows systems uncovered because the McAfee Agent is not compatible with one type of Linux operating system as well as niche operating systems. USCYBERCOM will include operational/functional/technical requirements to correct this with the requirements package sent to DISA, where feasible.

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

(~~FOUO~~) B.1. We recommend the Commander, U.S. Cyber Command:

- **(~~FOUO~~) a. Develop and submit requirements to the Defense Information Systems Agency to develop an automated method to determine whether DoD Components are appropriately configuring the Host Intrusion Prevention System on computer systems.**

USCYBERCOM agrees with this recommendation.

USCYBERCOM is working both future and current actions to address Host Intrusion Prevention System (HIPS) automation.

USCYBERCOM is currently addressing the HIPS automation to meet the recommendation by including all HIPS functional requirements, developed under/by the Enterprise Solutions Steering Group's technical arm – the Cyber Capabilities Working Group. The Cyber Capabilities Working Group will staff the functional and operational McAfee HIPS requirements to DISA by end of CY 11.

For future HIPS capabilities, the Cyber Capabilities Working Group has already established a second generation host-based security system (HBSS) requirements review. These 2nd generation host-based security capabilities and services requirements will be part of a new full and open acquisition, with a Request For Proposal due for release in September 2012, and will include Host Intrusion Prevention System measures.

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

- ~~(FOUO)~~ b. **Require DoD Components to report Host Intrusion Prevention System configuration information through the automated method, once the capability exists, referred to in recommendations B.1.a and B.2.**

USCYBERCOM agrees with this recommendation.

USCYBERCOM is working both future and current actions to address Host Intrusion Prevention System (HIPS) reporting.

USCYBERCOM is preparing a Task Order (TASKORD) to require DoD Components to generate reports, on a periodic basis, from their HBSS servers and submit them via email. The HBSS server can be configured to export and e-mail these reports automatically to ensure they are not modified in any way after leaving the server. This methodology will provide USCYBERCOM with more accurate configuration data, but it will not be fully automated. This is a near-term solution to gain better insight into current configurations while DISA works with McAfee on a more robust solution.

When a fully automated method becomes available, USCYBERCOM will release another TASKORD directing DoD Components to configure their HBSS servers to report configuration information utilizing an updated automated method.

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

~~(FOUO)~~ C. We recommend that the Commander, U.S. Cyber Command, review and update the list of Host Intrusion Prevention System signatures at least annually to ensure the signatures adequately protect DoD computer systems.

USCYBERCOM agrees with this recommendation.

A process has been developed for USCYBERCOM to provide McAfee with areas of concern for which they can select signatures from their inventory to address. The DISA Field Security Office will provide support by testing these select signatures to assess their effectiveness, potential for operational impact and make any necessary adjustments prior to fielding. Once the DISA review is complete, USCYBERCOM will issue a TASKORD to DoD Components for signature compliance. This process will recur monthly with new signatures added each month to continuously bolster DoD's defensive posture.

USCYBERCOM plans to mandate this signature application by the end of the first quarter of CY12. The signature list will be the minimum configuration requirements, and sites blocking additional signatures will be encouraged to maintain their own signatures as well to provide additional protection.

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

(~~FOUO~~) D.2. We recommend the Commander, U.S. Cyber Command, require DoD Components to roll up Unclassified but Sensitive Internet Protocol Router Network Host Based Security System event data once the capability exists to fully consolidate that data.

USCYBERCOM agrees with this recommendation.

Both DISA and COCOM/Service/Agency/Field Activity (CC/S/A/FA) configuration changes and supporting system acquisitions are required in order to collect HIPS incident data from NIPRNet hosts to meet this recommendation. Specifically, the system acquisitions would include intermediate roll-up servers owned and operated by the CC/S/A/FAs to process alert and asset information, and the configuration changes would include data reduction for consumption to the global tier servers. This is due to the sheer volume of data that is anticipated. Without a standardized, tiered reporting architecture with automated data flow control mechanisms in place, USCYBERCOM's data repository could quickly become saturated and unusable.

Further, Computer/Network Defense Service Providers (CNDSP) and CC/S/A/FAs will have to reconcile reporting responsibilities.

CNDSPs will need to build up their HBSS capabilities to handle NIPRNET alert reporting. DISA and USCYBERCOM will jointly release a data call to determine the state of HBSS and any additional required resources for each CNDSP to support full NIPRNET reporting. The data-call will be issued by end of 1st Qtr CY12 and used to understand implementation timelines.

With the HBSS capabilities of the CNDSP's properly assessed, limited data collection can begin through a pilot effort to implement automated reporting thresholds. The types of incident data collected can be expanded in a planned, phased manner as we increase our fidelity on the number and type of incident alerts being generated. We will focus on the most critical incidents first and expand our scope as we improve the ability and capacity to address incidents by degree of criticality.

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

Internal Control Weaknesses

USCYBERCOM did not have a reliable method to ensure that DoD Components appropriately configured HIPS on computer systems within DoD. USCYBERCOM relied on responses from DoD Components to determine whether they configured HIPS in accordance with USCYBERCOM requirements. Also, USCYBERCOM could not access and review NIPRNet HBSS event data because it appropriately focused first on obtaining SIPRNet HBSS event data.

USCYBERCOM agrees with these weaknesses.

USCYBERCOM is working near-, mid-, and long-term actions to address Host Intrusion Prevention System (HIPS) automated compliance review.

A near-term effort is underway to mandate DoD Components run a query on each of their Tier 3 HBSS servers periodically, aggregate the results through their CNDSPs, and provide results to USCYBERCOM. This is intended to replace manual VMS reporting and will guarantee the validity of the data being provided. These reports will be mandated by end of 1st Qtr CY 12 in conjunction with the publishing of a minimum HIPS policy.

A mid-term effort involves DISA and McAfee developing a way for these configuration metrics to be automatically fed through the DoD Components to USCYBERCOM without the need for any manual aggregation. USCYBERCOM will staff functional requirements for this automated reporting capability to DISA by the end of 1st Qtr CY12.

DISA and USCYBERCOM are addressing long-term compliance through the 2nd generation HBSS replacement, ref the answer to question B.1. These requirements will be released in an RFP during 3rd Qtr CY12.

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

RECOMMENDATIONS FOR OTHER AGENCIES:

(~~FOUO~~) B.2. We recommend the Director, Defense Information Systems Agency, develop the automated capability for U.S. Cyber Command to determine whether DoD Components are appropriately configuring the Host Intrusion Prevention System.

(~~FOUO~~) B.3. We recommend that the Director, Force Health Protection and Readiness:

- (~~FOUO~~) a. Enable Host Intrusion Prevention System application blocking on Windows Unclassified but Sensitive Internet Protocol Router Network servers.

- (~~FOUO~~) b. Configure Host Intrusion Prevention System application blocking to block the required blacklist items for Windows Unclassified but Sensitive Internet Protocol Router Network workstations and servers.

(~~FOUO~~) B.4. We recommend the Director, Defense Microelectronics Activity, configure application blocking for Windows Unclassified but Sensitive Internet Protocol Router Network servers in accordance with DoD guidance.

(~~FOUO~~) D.1. We recommend the Director, Defense Information Systems Agency, fully develop the capability to consolidate Unclassified but Sensitive Internet Protocol Router Network Host Based Security System event data to allow U.S. Cyber Command access to that data.

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

Defense Information Systems Agency Comments

DEFENSE INFORMATION SYSTEMS AGENCY
P. O. BOX 549
FORT MEADE, MARYLAND 20755-0549

IN REPLY REFER TO Program Executive Office for Mission Assurance (PEO-MA) 5 December 2011

MEMORANDUM FOR Inspector General, Department of Defense

SUBJECT: Response to DoD IG project number D2011-D000LB-0124.000 (8 November 2011)

1. The Defense Information Systems Agency, Director for Mission Assurance and Network Operations (PEO-MA), is responding as requested to DoD-IG recommendations B.2. and D.1. as noted in the report.

2. The responses outlined in Enclosure 1 summarize the actions that the Program Executive Office for Mission Assurance will take in regards to the recommendations of the DoD Inspector General.

3. Please contact either (b) (6) [redacted] should you have any questions.

(b) (6) [redacted]

1 Enclosure

MARK S. ORNDORFF
Director, Mission Assurance and
Network Operations

Enclosure 1

~~(FOUO)~~ **B.2.** *We recommend the Director, Defense Information Systems Agency, develop the automated capability for U.S. Cyber Command to determine whether DoD Components are appropriately configuring the Host Intrusion Prevention System.*

DISA PEO Response:

Concur - DISA acknowledges the DoD-IG recommendation to automate the status of HIPS configuration. DISA has delivered a local site capability to determine HIPS status of local end-points. This capability can be leveraged by exporting and emailing the report to USCYBERCOM. Efforts are ongoing to automate configuration and site status information, including HIPS configuration status, via the Secure Configuration Management (SCM) and Continuous Monitoring and Risk Scoring (CMRS) efforts. The full capability for automatic visualization of HIPS configuration data will be available in Q3 or Q4, 2014.

~~(FOUO)~~ **D.1.** *We recommend the Director, Defense Information Systems Agency, fully develop the capability to consolidate Unclassified but Sensitive Internet Protocol Router Network Host Based Security System event data to allow U.S. Cyber Command access to that data.*

DISA PEO Response:

Concur - DISA acknowledges the DoD-IG recommendation to develop the capability for the reporting of unclassified event data. DISA has an initial capability in place today. This capability will need an increase in capacity once the DoD order is given to report alerts to the NIPR SIEM. Additional requirements must be met with regard to command, control and communications as well as finalizing the OGS OPORD directives to implement the DoD reporting of unclassified data. DISA will continue to work with USCYBERCOM to ensure that the technical solution meets the operational intent.

Defense Microelectronics Activity Comments

DEFENSE MICROELECTRONICS ACTIVITY
4234 54th STREET
MCCLELLAN, CALIFORNIA 95652-2100

December 8, 2011

MEMORANDUM FOR DOD INSPECTOR GENERAL

SUBJECT: (U) Improvements Needed With Host-Based Intrusion Detection Systems (Project No. D2011-DOOOLB-0124.000)

(U//~~FOUO~~) We have reviewed the subject report and concur with its findings and recommendations as they apply to the Defense Microelectronics Activity (DMEA). To ensure compliance with stated DoD requirements, as recommended by the subject DoDIG report; DMEA is exercising the following corrective actions:

1. Assess DoDIG findings and recommendations; and develop mitigation strategy to correct deficiencies. (Completed)
2. Analyze DISA's recommended Application Blocking methodology, as provided by the DoDIG staff during their visit to DMEA. (Completed)
3. Correlate current list of DMEA trusted applications to the recommended Application Blocking methodology; and develop new DMEA specific HIPS Application Blocking rule set. (Completed)
4. Test new Application Blocking rule set to ensure compliance with the recommended Application Blocking methodology. (Completed)
5. Deploy new Application Blocking rule set to all DMEA Windows NIPRNet servers. (In Process: Currently deployed to 8 of 34 servers)

(U//~~FOUO~~) Based on corrective actions taken to date, DMEA is expected to be fully compliant with the subject report's recommendations regarding the implementation of HIPS Application Blocking requirements on its Windows NIPRNet servers no later than 20 January, 2012.

(U) We wish to thank the DODIG team for their assistance during their visit to DMEA; and for the help provided following that visit. Should you have any questions please direct them to me a[(b) (6)]

[(b) (6)]

James M. Dininger
Deputy Director
Defense Microelectronics Activity

~~FOR OFFICIAL USE ONLY~~

Inspector General
Department of Defense

~~FOR OFFICIAL USE ONLY~~