

CHUCK GRASSLEY, IOWA, CHAIRMAN

MIKE CRAPO, IDAHO
PAT ROBERTS, KANSAS
MICHAEL B. ENZI, WYOMING
JOHN CORNYN, TEXAS
JOHN THUNE, SOUTH DAKOTA
RICHARD BURR, NORTH CAROLINA
JOHNNY ISAKSON, GEORGIA
ROB PORTMAN, OHIO
PATRICK J. TOOMEY, PENNSYLVANIA
TIM SCOTT, SOUTH CAROLINA
BILL CASSIDY, LOUISIANA
JAMES LANKFORD, OKLAHOMA
STEVE DAINES, MONTANA
TODD YOUNG, INDIANA

RON WYDEN, OREGON
DEBBIE STABENOW, MICHIGAN
MARIA CANTWELL, WASHINGTON
ROBERT MENENDEZ, NEW JERSEY
THOMAS R. CARPER, DELAWARE
BENJAMIN L. CARDIN, MARYLAND
SHERROD BROWN, OHIO
MICHAEL F. BENNET, COLORADO
ROBERT P. CASEY, JR., PENNSYLVANIA
MARK R. WARNER, VIRGINIA
SHELDON WHITEHOUSE, RHODE ISLAND
MAGGIE HASSAN, NEW HAMPSHIRE
CATHERINE CORTEZ MASTO, NEVADA

United States Senate

COMMITTEE ON FINANCE

WASHINGTON, DC 20510-6200

KOLAN DAVIS, STAFF DIRECTOR AND CHIEF COUNSEL
JOSHUA SHEINKMAN, DEMOCRATIC STAFF DIRECTOR

April 9, 2019

VIA ELECTRONIC TRANSMISSION

The Honorable Alex Azar II
Secretary
Department of Health and Human Services

Dear Secretary Azar:

The Presidential Policy Directive on Critical Infrastructure Security and Resilience (PPD-21), tasked Federal entities with strengthening the security and resiliency of critical infrastructure against physical and cyber threats.¹ The Department of Health and Human Services was designated to oversee and manage the health care and public health sectors in this regard.² In 2017, the Health Care Industry Cybersecurity (HCIC) Task Force identified the need to “[i]ncrease the security and resilience of medical devices and health IT” and “ensure cyber security awareness and education” in order to keep patients safe and protect their information from vulnerability or exploitation.³ Cyber risks to the health care sector are real and increasing, and all reasonable efforts must be taken to combat them to protect individuals and their privacy.

On March 1, 2019, the Department of Health and Human Services Office of Inspector General (HHS OIG) released a report entitled, “Summary Report for Office of Inspector General Penetration Testing of Eight HHS Operating Division Networks.”⁴ That report outlined the results of penetration testing of the Centers for Disease Control, National Institutes of Health, Indian Health Service, Health and Human Services Office of the Secretary, Substance Abuse and Mental Health Services Administration, Centers for Medicare and Medicaid Services, Food and Drug Administration, and Administration for Children and Families. These cyber tests took place during fiscal years 2016 and 2017 and were conducted by Defense Point Security (DPS) on

¹ See Press Release, The White House, Presidential Policy Directive -- Critical Infrastructure Security and Resilience, PPD-21 (Feb. 12, 2013).

² *Id.*

³ Health Care Industry Cybersecurity (HCIC) Task Force, *Report On Improving Cybersecurity In The Health Care Industry*, at 21 (June 2017), available at <https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf>.

⁴ U.S. DEP’T OF HEALTH AND HUMAN SERV., OFFICE OF INSPECTOR GEN., A-18-18-08500, SUMMARY REPORT FOR OFFICE OF INSPECTOR GENERAL PENETRATION TESTING OF EIGHT HEALTH AND HUMAN SERVICES OPERATING DIVISION NETWORKS (2019).

behalf of HHS OIG.⁵ These tests probed and analyzed the cyber posture and vulnerability from outside of the HHS Operating Division's (HHS OpDiv) network security perimeter.⁶

The report uncovered some critical deficiencies and issues where HHS has room for improvement. Specifically, the HHS OIG report stated the likely level of sophistication needed by a prospective attacker to successfully infiltrate HHS OpDiv networks is low to moderate and does not require significant technical knowledge.⁷ In addition, during testing the HHS OIG identified 197 vulnerabilities to include 37 classified as Critical, 36 High, 116 Medium, and 8 as low.⁸ Moreover, HHS OIG "[was] able to gain access to various devices on the network, escalate privileges, evade detection, and gain unauthorized access to personally identifiable information (PII) at four of the eight OPDIVs that we tested."⁹ In gaining that access, the penetrations were able to access personally identifiable information for more than 9,000 records, which included phone numbers, address information, case information, and some photographs.¹⁰ Further, HHS OIG found that "[v]ery little of our penetration testing activity was detected by HHS OpDiv monitoring controls."¹¹

HHS OIG issued several recommendations which include the use of standard security requirements, requiring contractors to comply with appropriate security standards, and improving continuous monitoring procedures.¹² While the HHS Office of Information Security (OIS) concurred with the recommendations, I would like clarification on what HHS has done to achieve these objectives.

Cyberattacks on our government systems are an emerging threat that foreign governments and other entities seek to leverage for their benefit.¹³ Such serious vulnerabilities in protecting sensitive formation erodes the public's confidence in these systems. The Department must take immediate, sustained, and effective action to reduce and eliminate these threats and better protect its systems.

⁵ *Id.* at 1.

⁶ *Id.* at 11.

⁷ *Id.* at 17.

⁸ *Id.* at 16 (noting that the Common Vulnerability Scoring System (CVSS) was used to measure the vulnerabilities). *See e.g.*, National Vulnerability Database, available at <https://nvd.nist.gov/vuln-metrics/cvss>.

⁹ *Id.* at 17.

¹⁰ *Id.* at 21.

¹¹ *Id.* at 17.

¹² Response to Request for Additional Information from Memo, submitted December 19, 2018, OCIO Comments on OIG Report A-18-18-08500, entitled, SUMMARY REPORT OF OFFICE OF INSPECTOR GENERAL PENETRATION TESTING OF EIGHT HHS OPERATING DIVISION NETWORKS.

¹³ *See* Letter from Hon. Charles E. Grassley, Chairman, Senate Judiciary Comm., to Hon. Francis Collins, Director, National Institutes of Health (Oct. 23, 2018); *see also* Letter from Hon. Charles E. Grassley, Chairman, Senate Judiciary Comm., to Hon. Jeff Sessions, Attorney General, U.S. Department of Justice (Sept. 19, 2018).

Accordingly, please provide written responses to the following questions no later than April 23, 2019:

1. Which HHS departments were notified via early alerts about the HHS OIG's findings?
 - a. On what date(s) were the HHS departments notified of the early alerts?
 - b. What actions were taken to address the issues raised in the early alerts?
2. Has HHS implemented any new agency-wide cyber policies to address concerns raised in the HHS OIG report? If so, what are they and when were they implemented?
3. With respect to the HHS OIG recommendations, please provide the Committee a written summary, on a rolling basis if necessary, describing how HHS has implemented fixes sufficient to close the recommendations.¹⁴
4. Please provide the Committee a timeline outlining the implementation of the recommended policies and anticipated dates of compliance.

In addition to answering the aforementioned questions, please provide a briefing to my staff no later than April 30, 2019, regarding the steps you have taken, or plan to take, to address the concerns raised by the HHS OIG report. I anticipate that your written reply and most responsive documents will be unclassified. Please send all unclassified material directly to the Committee. In keeping with the requirements of Executive Order 13526, if any of the responsive documents do contain classified information, please segregate all unclassified material within the classified documents, provide all unclassified information directly to the Committee, and provide a classified addendum to the Office of Senate Security. Although the Committee complies with all laws and regulations governing the handling of classified information, it is not bound, absent its prior agreement, by any handling restrictions.

Thank you in advance for your prompt attention to these matters. Should you have any questions, please contact Josh Flynn-Brown of my Committee staff at (202) 224-4515.

Sincerely,



Charles E. Grassley
Chairman
Committee on Finance

Enclosures: Redacted March 1, 2019, HHS OIG Report

¹⁴ See Response to Request for Additional Information from Memo, *supra* n. 12, at 1.



DEPARTMENT OF HEALTH AND HUMAN SERVICES

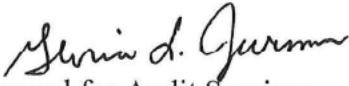
OFFICE OF INSPECTOR GENERAL

WASHINGTON, DC 20201



MAR - 1 2019

TO: Ed Simcox
Acting Chief Information Officer
HHS Office of the Secretary

FROM: Gloria L. Jarmon 
Deputy Inspector General for Audit Services

SUBJECT: Summary Report for Office of Inspector General Penetration Testing of Eight HHS Operating Division Networks (A-18-18-08500)

The attached summary report provides the results of our penetration testing audits across eight HHS Operating Division networks: CDC, NIH, IHS, HHS OS, SAMHSA, CMS, FDA, and ACF.

This report contains restricted, sensitive information that may be exempt from release under the Freedom of Information Act, 5 U.S.C. § 552. The report will not be posted on the Internet. If information in the report is released pursuant to a request under the Act, the restricted, sensitive information and other information exempt from release will be redacted. However, a modified version of the Report in Brief will be posted on the OIG Web site at <https://oig.hhs.gov> which omits details that could compromise the security of HHS systems or data.

If you have any questions or comments about this report, please do not hesitate to call me, or your staff may contact Jarvis Rodgers, Director, Cybersecurity and Information Technology Audit Division, at [REDACTED]. We look forward to receiving your final management decision within 6 months. Please refer to report number A-18-18-08500 in all correspondence.

Attachment

***Warning—This report contains restricted information for official use.
Distribution is limited to authorized officials.***

Department of Health and Human Services

**OFFICE OF
INSPECTOR GENERAL**

**SUMMARY REPORT FOR OFFICE
OF INSPECTOR GENERAL
PENETRATION TESTING OF
EIGHT HHS OPERATING
DIVISION NETWORKS**

WARNING: THIS REPORT CONTAINS RESTRICTED, SENSITIVE INFORMATION, SUCH AS CONFIDENTIAL PROPRIETARY MATERIAL WITH A HIGH POTENTIAL FOR MISUSE. DISTRIBUTION SHOULD BE STRICTLY LIMITED. DO NOT REPRODUCE OR RELEASE TO ANY PERSON WITHOUT THE PRIOR APPROVAL OF THE OFFICE OF AUDIT SERVICES.



**Gloria L. Jarmon
Deputy Inspector General
for Audit Services**

**March 2019
A-18-18-08500**

Office of Inspector General

<https://oig.hhs.gov>

The mission of the Office of Inspector General (OIG), as mandated by Public Law 95-452, as amended, is to protect the integrity of the Department of Health and Human Services (HHS) programs, as well as the health and welfare of beneficiaries served by those programs. This statutory mission is carried out through a nationwide network of audits, investigations, and inspections conducted by the following operating components:

Office of Audit Services

The Office of Audit Services (OAS) provides auditing services for HHS, either by conducting audits with its own audit resources or by overseeing audit work done by others. Audits examine the performance of HHS programs and/or its grantees and contractors in carrying out their respective responsibilities and are intended to provide independent assessments of HHS programs and operations. These assessments help reduce waste, abuse, and mismanagement and promote economy and efficiency throughout HHS.

Office of Evaluation and Inspections

The Office of Evaluation and Inspections (OEI) conducts national evaluations to provide HHS, Congress, and the public with timely, useful, and reliable information on significant issues. These evaluations focus on preventing fraud, waste, or abuse and promoting economy, efficiency, and effectiveness of departmental programs. To promote impact, OEI reports also present practical recommendations for improving program operations.

Office of Investigations

The Office of Investigations (OI) conducts criminal, civil, and administrative investigations of fraud and misconduct related to HHS programs, operations, and beneficiaries. With investigators working in all 50 States and the District of Columbia, OI utilizes its resources by actively coordinating with the Department of Justice and other Federal, State, and local law enforcement authorities. The investigative efforts of OI often lead to criminal convictions, administrative sanctions, and/or civil monetary penalties.

Office of Counsel to the Inspector General

The Office of Counsel to the Inspector General (OCIG) provides general legal services to OIG, rendering advice and opinions on HHS programs and operations and providing all legal support for OIG's internal operations. OCIG represents OIG in all civil and administrative fraud and abuse cases involving HHS programs, including False Claims Act, program exclusion, and civil monetary penalty cases. In connection with these cases, OCIG also negotiates and monitors corporate integrity agreements. OCIG renders advisory opinions, issues compliance program guidance, publishes fraud alerts, and provides other guidance to the health care industry concerning the anti-kickback statute and other OIG enforcement authorities.

Notices

THIS REPORT CONTAINS RESTRICTED INFORMATION

This report should not be reproduced or released to any other party without specific written approval from OAS.

OFFICE OF AUDIT SERVICES FINDINGS AND OPINIONS

The designation of financial or management practices as questionable, a recommendation for the disallowance of costs incurred or claimed, and any other conclusions and recommendations in this report represent the findings and opinions of OAS. Authorized officials of the HHS operating divisions will make final determination on these matters.

Report in Brief

Date: March 2019

CIN: A-18-18-08500

U.S. DEPARTMENT OF HEALTH & HUMAN SERVICES
OFFICE OF INSPECTOR GENERAL



Why OIG Did This Review

We conducted a series of OIG audits at eight HHS Operating Divisions (OPDIVs) using network and web application penetration testing to determine how well HHS systems were protected when subject to cyberattacks.

Our objectives were to determine whether security controls were effective in preventing certain cyberattacks, the likely level of sophistication an attacker needs to compromise systems or data, and the HHS OPDIV's ability to detect attacks and respond appropriately.

How OIG Did This Review

During Fiscal Years 2016 and 2017, we conducted tests at eight HHS OPDIVs. We contracted with Defense Point Security (DPS) to provide knowledgeable subject matter experts to conduct the penetration testing on behalf of OIG. We closely oversaw the work performed by DPS and testing was performed in accordance with generally accepted government auditing standards and agreed-upon Rules of Engagement between OIG and the OPDIVs.

Summary Report for Office of Inspector General Penetration Testing of Eight HHS Operating Division Networks

What OIG Found

On the basis of the systems we tested, we determined that security controls across the eight HHS OPDIVs needed improvement to more effectively detect and prevent certain cyberattacks. During testing, we identified a total of 197 vulnerabilities, of which 37 were classified Critical, 36 High, 116 Medium, and 8 Low. We were able to gain access to various devices on the network, escalate privileges, evade detection, and gain unauthorized access to personally identifiable information at four of the eight OPDIVs we tested.

We promptly shared significant preliminary findings with the OPDIVs during the course of the audits and provided separate reports with the detailed results to each OPDIV after testing was completed. We would like to thank HHS and its OPDIVs for the cooperation we received throughout the penetration testing.

What OIG Recommends and HHS's Comments

We recommend that HHS:

- [REDACTED] (b)(7)F standard established by HHS;
- ensure all future web application developments incorporate security requirements from an industry recognized web application security standard;
- ensure all future web application development contractors include appropriate procurement provisions that outline application security standards and procedures that must be adhered to during development and throughout the System Development Life Cycle; and
- [REDACTED] (b)(7)F other mechanisms that are in place to monitor and test for internal cybersecurity vulnerabilities.

In written comments to our draft report, HHS concurred with our four recommendations and described actions it has taken or plans to take to address our findings.

*Warning—This report contains restricted information for official use.
Distribution is limited to authorized officials.*



Summary Report for Office of Inspector General Penetration Testing of Eight HHS Operating Division Networks

CIN: A-18-18-08500

February 2019





Topics

- Overview and Background
- Objectives and Scope
- Methodology
- What We Found
- Vulnerabilities
- Security Posture Ranking Based On Operating Division (OPDIV) Results
- How did the Office of Inspector General (OIG) Breach Eight OPDIVs?
- Common Root Causes





Topics

- What the Department of Health and Human Services (HHS) should be doing to prevent these types of attacks
- OIG Recommendations
- Applicable NIST Criteria
- OIG Penetration Test Reports
- Acronyms
- HHS Comments





Overview

This summary report will:

- provide actionable information regarding HHS's cyber-security posture,
- provide information on common vulnerabilities across OPDIVs, and
- provide recommendations and strategies to mitigate exploited weaknesses.





Background

The HHS OIG conducted a series of penetration testing audits focused on network and web application vulnerabilities.





Background

Penetration testing was performed at eight OPDIVs (in the order below):

FY 2016	<ul style="list-style-type: none"> • Centers for Disease Control and Prevention (CDC) • National Institutes of Health (NIH) • Indian Health Service (IHS) • Office of the Secretary (OS)
FY 2017	<ul style="list-style-type: none"> • Substance Abuse and Mental Health Services Administration (SAMHSA) • Centers for Medicare & Medicaid Services (CMS) • Food and Drug Administration (FDA) • Administration for Children and Families (ACF)





Background

A well-designed program of proactive threat hunting and regularly scheduled network and vulnerability scanning interspersed with periodic penetration testing can help prevent many types of attacks and reduce the potential damaging effects of successful ones.





Objectives

Our objectives were to determine:

- whether security controls were effective in preventing certain cyberattacks,
- the likely level of sophistication an attacker needs to compromise systems or data, and
- the OPDIV's ability to detect attacks and respond appropriately.





Scope

Our scope included the OPDIV's network infrastructure used to support its applications and other resources. We tested core network devices (e.g., routers, firewalls, switches), workstations, servers, and other resources connected to the infrastructure.





Methodology: Use of Specialists

To assist with the series of audits, we relied on testing performed by Defense Point Security (DPS). DPS provided subject matter experts throughout all phases of the testing: external, internal, social engineering, and wireless testing.

OIG closely oversaw the DPS work to ensure that all objectives were met and that testing was performed in accordance with government auditing standards, as well as the agreed-upon Rules of Engagement.





Methodology: External Testing

External security testing was conducted from outside the OPDIV's network perimeter. This type of testing offers the ability to view the environment's security posture as it appears outside the security perimeter—usually as seen from the internet—with the goal of revealing vulnerabilities that an external attacker could exploit (performed at eight OPDIVs).

No special privilege or prior system information was provided to testers other than external Internet Protocol (IP) addresses.





Methodology: Internal Testing

Internal security testing was performed from inside the OPDIV's network perimeter and assumed the identity of a trusted insider or an attacker who had penetrated the perimeter defenses (performed at seven OPDIVs, OS was excluded due to the procurement window for testing).

Testers came on-site to OPDIV office location(s) or data center(s). Other than building access, no special privileges were provided to testers.

Minimal system information was provided (IPs/exclusions).





Methodology: Social Engineering

Limited social engineering (email phishing) attacks were performed on targeted employees in an attempt to trick OPDIV employees into opening malicious file attachments. [REDACTED] (b)(7)F

[REDACTED] (b)(7)F

[REDACTED] (b)(7)F

We performed social engineering attacks at seven OPDIVs (OS excluded).



Warning—This report contains restricted information for official use. Distribution is limited to authorized officials.

13



Methodology: Wireless Testing

Wireless cyberattacks were performed using tools and techniques commonly used by attackers to gain unauthorized access to wireless networks and sensitive data (performed at seven OPDIVs, OS excluded).

Discovered possible methods of attack, such as intercepting wireless communications, to gain unauthorized access or eavesdrop on wireless communications.





Methodology: Adherence to GAGAS

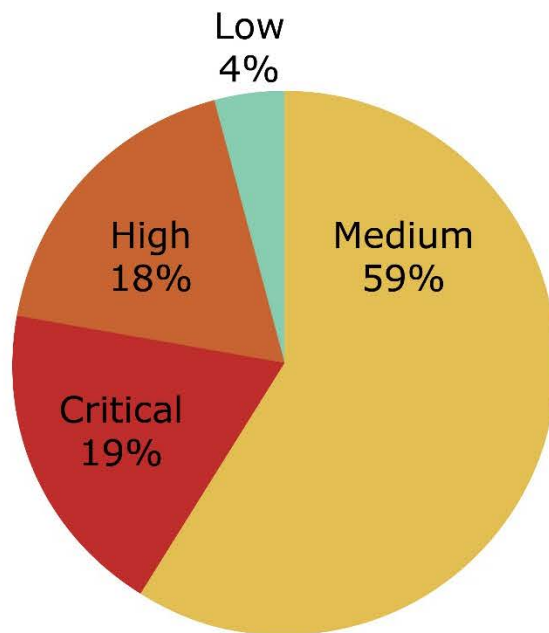
We conducted this performance audit in accordance with GAGAS. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.





What We Found

During testing, we identified a total of 197 vulnerabilities, of which, 37 were classified* Critical, 36 High, 116 Medium, and 8 Low.



*Common Vulnerability Scoring System 3.0 calculator was used to derive ratings.





What We Found

Overall, based on the successful exploits, we considered the likely level of sophistication needed by an attacker to exploit HHS OPDIV systems as low to moderate, meaning the attacks did not require significant technical knowledge in order to exploit, but many were also not publicly known vulnerabilities.

Very little of our penetration testing activity was detected by HHS OPDIV monitoring controls. [REDACTED] (b)(7)F

[REDACTED] (b)(7)F

We were able to gain access to various devices on the network, escalate privileges, evade detection, and access personally identifiable information (PII) at four of the eight OPDIVs we tested.



Warning—This report contains restricted information for official use. Distribution is limited to authorized officials.



We Found PII

(b)(7)F

(b)(7)F

(b)(7)F

employee and contractor PII, including full name, title, office, location, phone number, and direct supervisor.

(b)(7)F

by searching using either part of their name or the city in which they work.



Warning—This report contains restricted information for official use. Distribution is limited to authorized officials.

18



We Found PII

(b)(7)F

(b)(7)F



Warning—This report contains restricted information for official use. Distribution is limited to authorized officials.



We Found PII

(b)(7)F

We entered malicious database queries into certain publicly-accessed (b)(7)F websites and were able to expose PII, including full names, contact information, security questions, and answers. (b)(7)F

(b)(7)F

(b)(7)F



Warning—This report contains restricted information for official use. Distribution is limited to authorized officials.



We Found PII

(b)(7)F

(b)(7)F server, contained PII about (b)(7)F such as full name, age, (b)(7)F (b)(7)F date of birth, and other sensitive information. We were able to access PII for more than 9,000 records. We also identified numerous case files containing PII, which included phone numbers, address information, case information, and photographs of the (b)(7)F for more than 3,000 case files.

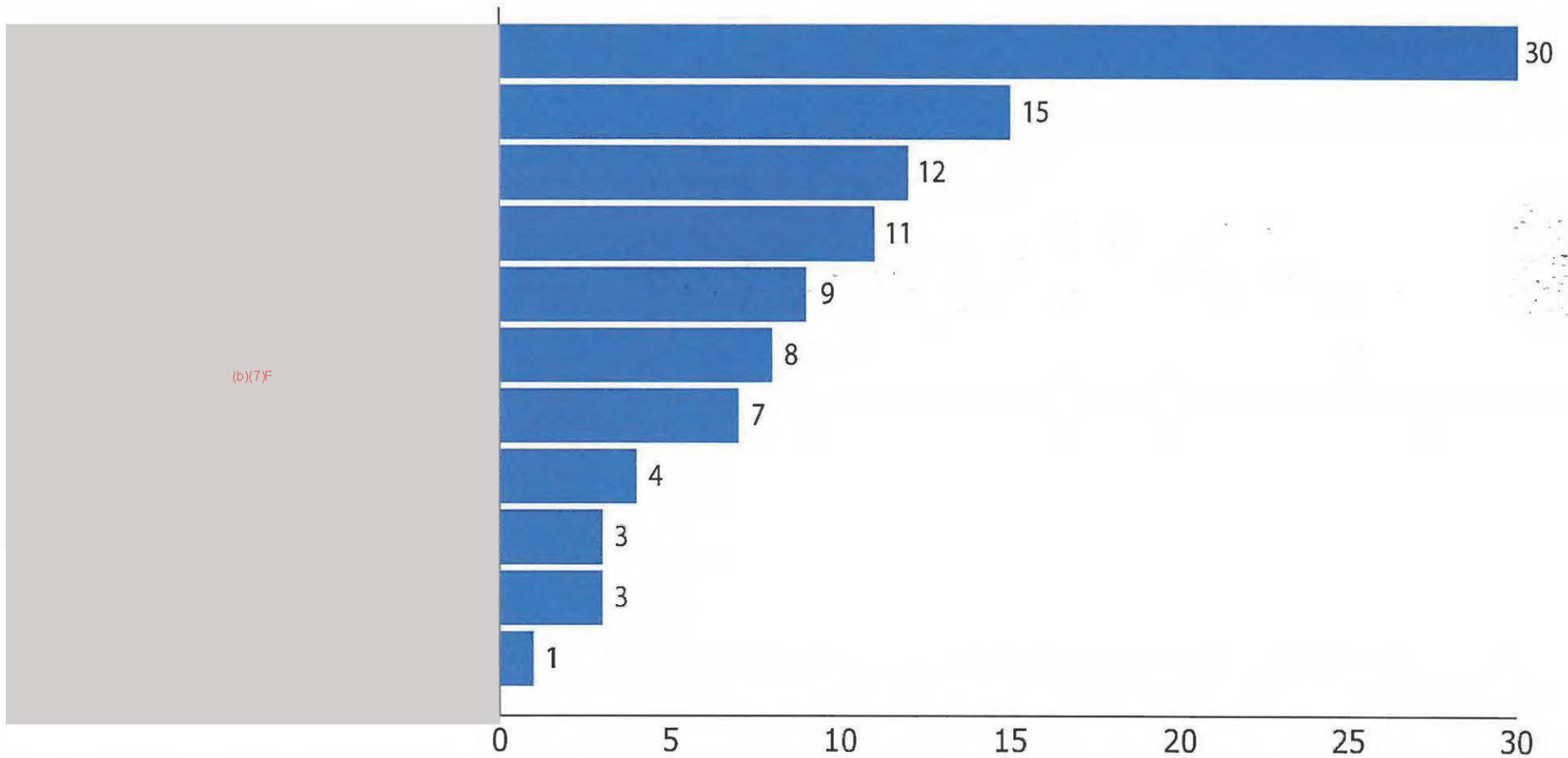
(b)(7)F



Warning—This report contains restricted information for official use. Distribution is limited to authorized officials.



Vulnerabilities: CDC, IHS, NIH, OS



Warning—This report contains restricted information for official use. Distribution is limited to authorized officials.



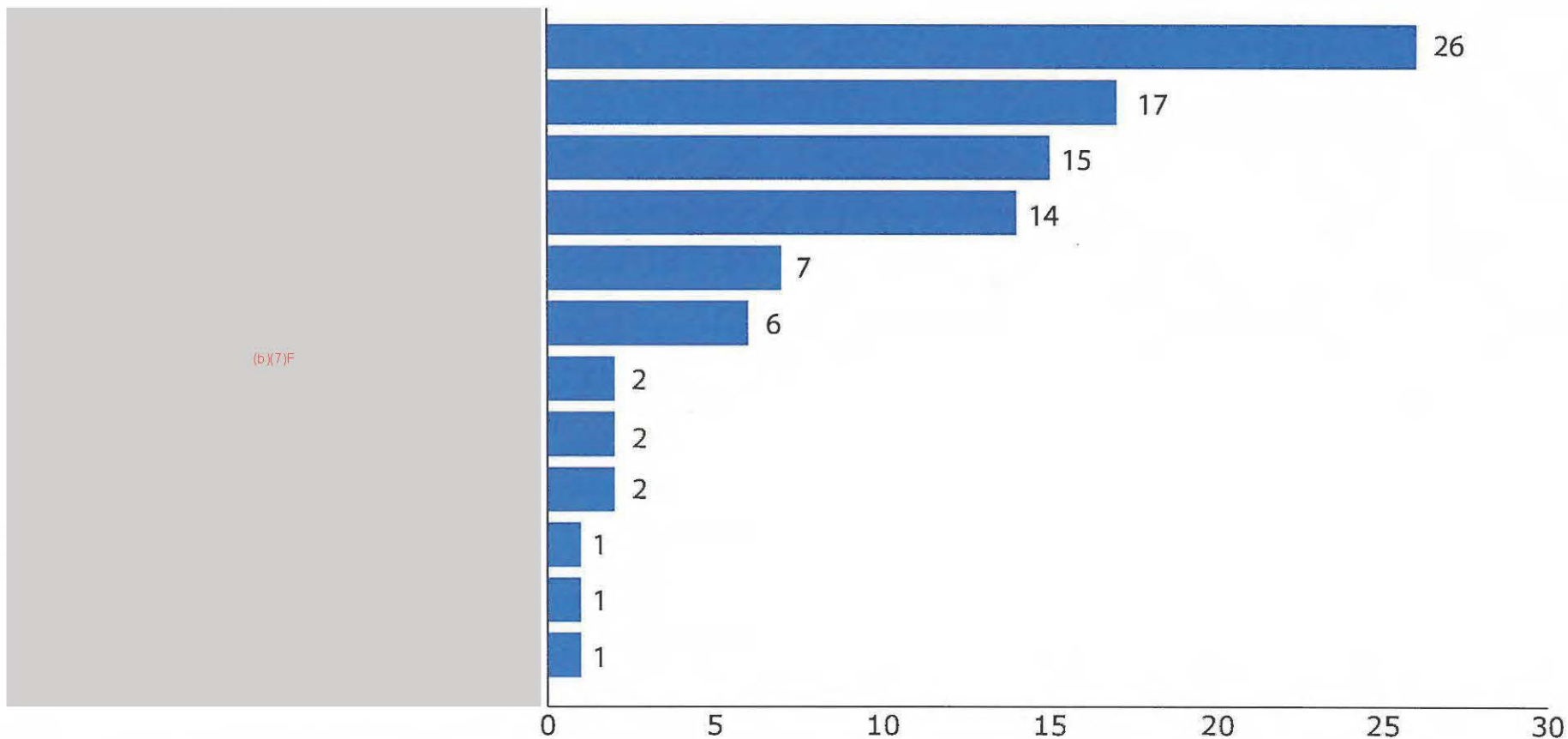
Vulnerabilities: CDC, IHS, NIH, OS

Vulnerability	CDC	IHS	NIH	OS
(b)(7)F	X	X	X	X
	X	X	X	
	X	X	X	X
		X	X	
		X		
	X	X	X	X
	X	X	X	
	X	X	X	
	X	X		X
		X	X	
	X	X	X	X

Warning—This report contains restricted information for official use. Distribution is limited to authorized officials.



Vulnerabilities: SAMHSA, CMS, FDA, ACF



Warning—This report contains restricted information for official use. Distribution is limited to authorized officials.



Vulnerabilities: SAMHSA, CMS, FDA, ACF

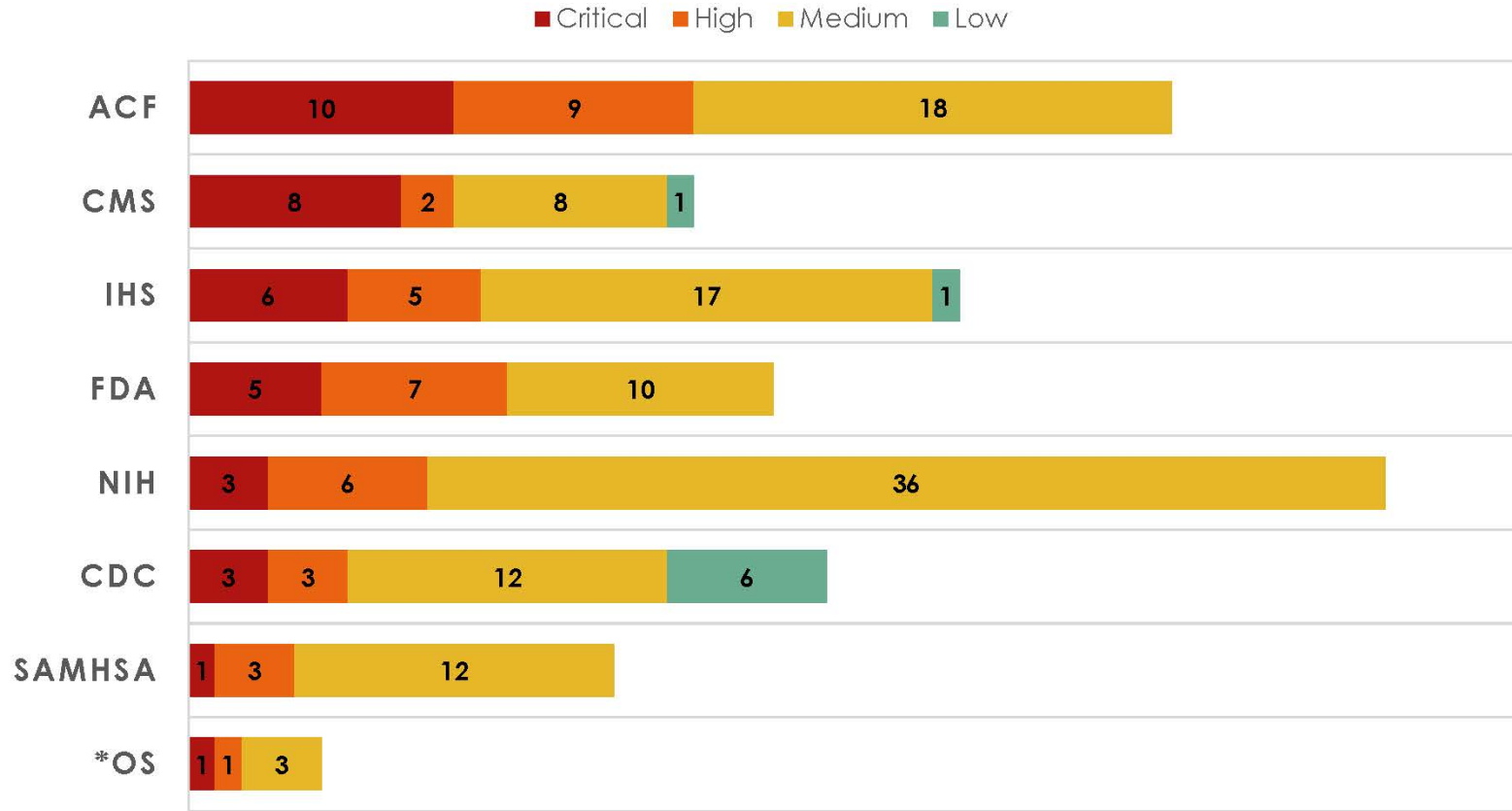
Vulnerability	ACF	CMS	FDA	SAMHSA
(b)(7)F		X		
			X	
			X	
	X			X
			X	
			X	X
			X	X
	X		X	X
	X	X	X	X
	X	X	X	X
	X	X	X	X
	X	X	X	X



Warning—This report contains restricted information for official use. Distribution is limited to authorized officials.



Security Posture Ranking Based On OPDIV Results



* OIG only performed external testing at the Office of the Secretary (OS).





How did OIG breach eight Operating Divisions, circumvent millions of dollars in HHS security controls, and evade detection?





Primary Techniques

(b)(7)F



Warning—This report contains restricted information for official use. Distribution is limited to authorized officials.



Common Root Causes

The common root causes of the vulnerabilities were:

-
-
-
-



Overall, the vulnerabilities OIG identified can be mitigated and/or eliminated by integrating cybersecurity during the development phase and monitoring cybersecurity controls throughout the system development life cycle.



Warning—This report contains restricted information for official use. Distribution is limited to authorized officials.



What HHS should be doing to prevent these types of attacks





OIG Recommendations

Ensure OPDIVs implement properly-configured [REDACTED] (b)(7)F in accordance with an agreed-upon baseline standard established by HHS.

Ensure all future web application developments incorporate security requirements from an industry recognized web application security standard (*e.g., Open Web Application Security Project (OWASP) and SystemAdmin, Audit, Network and Security (SANS)*).

Ensure all future web application development contractors include appropriate procurement provisions that outline application security standards and procedures that must be adhered to during development and throughout the system development life cycle.

Improve continuous monitoring procedures and require OPDIVs to test for [REDACTED] (b)(7)F [REDACTED] (b)(7)F as part of the Assessment and Authorizations process, system risk assessments, Office of Management and Budget A-123 reviews, follow-up testing for Plan of Action and Milestones, and other mechanisms that are in place to monitor and test for internal cybersecurity vulnerabilities.



Warning—This report contains restricted information for official use. Distribution is limited to authorized officials.



Applicable NIST Criteria

NIST SP 800-122: Guide to Protecting the Confidentiality of PII

NIST SP 800-45, version 2: Guidelines on Electronic Mail Security

NIST SP 800-132: Recommendation for Password-Based Key Derivation
Part 1: Storage Applications

NIST SP 800-40: Guide to Enterprise Patch Management Technologies

NIST SP 800-44, version 2: Guidelines on Securing Public Web Servers

NIST SP 800-53, revision 4: Security and Privacy Controls for Federal Information
Systems and Organizations

NIST SP 800-97: Establishing Wireless Robust Security Networks: A Guide to IEEE
802.11i





OIG Penetration Test Reports

2016 CDC Pen Test Report (A-18-15-30500)

2016 NIH Pen Test Report (A-18-15-30600)

2016 IHS Pen Test Report (A-18-16-30800)

2016 OS Pen Test Report (A-18-16-30900)

2017 SAMHSA Pen Test Report (A-18-16-30810)

2017 CMS Pen Test Report (A-18-17-08200)

2017 FDA Pen Test Report (A-18-17-08300)

2017 ACF Pen Test Report (A-18-17-08400)





Acronyms

- **XSS:** Cross-Site Scripting
- **GAGAS:** Generally Accepted Government Auditing Standards
- **OWASP:** Open Web Application Security Project
- **NIST:** National Institute of Standards and Technology
- **SANS:** SysAdmin, Audit, Network, and Security
- **URL:** Uniform Resource Locator; a set of strings to define a webpage location e.g., <https://www.oig.hhs.gov>





DEPARTMENT OF HEALTH & HUMAN SERVICES

Office of the Secretary

Office of the Chief Information Officer
Assistant Secretary for Administration
Washington, D.C. 20201

TO: Gloria Jarmon
Deputy Inspector General for Audit Services

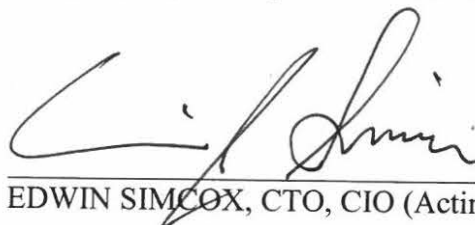
FROM: Ed Simcox
Acting Chief Information Officer
HHS Office of the Secretary

SUBJECT: Comments on OIG Report Entitled "Summary Report for Office of Inspector General Penetration Testing of Eight HHS Operating Division Networks (A-18-18-08500)"

Thank you for sharing the Summary Report on Penetration Testing at HHS Operating Divisions. The report covers activities during Fiscal Years 2016 and 2017. During these audits, the Operating Divisions (OpDivs) were able to address findings provided to them in "Spot Reports" on an immediate basis. The OpDivs have also incorporated actions to address their findings through the course of patching and upgrade activities of operation and maintenance. We take these findings very seriously, and have worked with the OpDivs on their resolution.

We are especially concerned about the findings that were classified as "Critical" or "High" and will follow up with the OpDivs to ensure that these have all been addressed. The recommendations provided in the report will be shared with the OpDivs, and discussed through our ongoing communications. While in-and-of itself, a finding may appear to be classified as a lower risk, we take your report seriously, as multiple findings may infer a greater risk when combined together. We also note that the findings themselves may lead us to look into Information Technology management practices where the implication of similar findings across OpDivs could be implied.

We appreciate the opportunity to review the Summary report, and hope that we can count on your partnership going forward.



EDWIN SIMCOX, CTO, CIO (Acting)



OFFICE OF THE
CHIEF INFORMATION OFFICER
 DEPARTMENT OF HEALTH AND HUMAN SERVICES

January 17, 2019

To: Jarvis Rodgers
 IT Audit Director, Cybersecurity and Information Technology Audit Division
 Office of Audit Services

Don Patterson
 Assistant Director, Cybersecurity and Information Technology Audit Division
 Office of Audit Services

From: Janet Vogel
 Chief Information Security Officer, Acting
 Office of Information Security

Subject: Response to Request for Additional Information from Memo submitted December 19, 2018, *OCIO Comments on OIG Report Entitled "Summary Report of Office of Inspector General Penetration Testing of Eight HHS Operating Division Networks (A-18-18-08500)"*

This memo is to provide additional information regarding activities in response to the HHS Office of Inspector General (OIG) report on *General Penetration Testing of HHS OpDivs*, which provided four (4) OIG recommendations. The HHS Office of Information Security (OIS) concurs with the recommendations and commits to taking the actions listed below.

OIG Recommendation 1 – [REDACTED] (b)(7)F
 [REDACTED] (b)(7)F : standard established by HHS.

OIS Actions –

1. OIS, in collaboration with the relevant Divisions within the Office of the Chief Information Officer (OCIO), has identified the following existing policies that pertain to this recommendation. OIS will assess the policies and provide updates as appropriate.
 - Minimum Security Configurations Standards Guidance,
 - HHS Minimum Security Configuration Standards for Palo Alto Networks,
 - Policy for Software Development Secure Coding Practices (draft is in clearance process),
 - Policy for Domain Name System (DNS) and Domain Name System Security Extensions Services (DNSSEC) (draft is in clearance process)
2. OIS will work with each OpDiv to ensure [REDACTED] (b)(7)F findings are documented and remediated, consistent with the HHS Plan of Action and Milestones (POA&M) requirements. OIS will review progress and maintenance on a regular basis.



OFFICE OF THE CHIEF INFORMATION OFFICER

DEPARTMENT OF HEALTH AND HUMAN SERVICES

OIG Recommendation 2 – Ensure all future web application developments incorporate security requirements from an industry recognized web application security standard (e.g., Open Web Application Security Project (OWASP) and SystemAdmin, Audit, Network and Security (SANS)).

OIS Actions –

1. OIS, in collaboration with the relevant Divisions within the OCIO, has identified the following existing policies that pertain to this recommendation. OIS will also explore the development of new policies, standards or memoranda as needed, and periodically review OpDiv compliance.
 - Minimum Security Configurations Standards Guidance,
 - Policy for Software Development Secure Coding Practices (draft is in clearance process),
 - HHS Policy for Web and Email Security (draft is in clearance process)
2. OIS will work with each OpDiv to ensure that these findings are remediated, consistent with the HHS POA&M requirements. Per these requirements, OpDivs will be required to identify remediation activities, timeframes, and resources required to address audit findings. OIS will review progress on a regular basis.

OIG Recommendation 3 – Ensure all future web application development contractors include appropriate procurement provisions outlining application security standards and procedures that must be adhered to during development and throughout the System Development Life Cycle.

OIS Actions –

1. OIS, in collaboration with the relevant Divisions within the OCIO, has identified the following existing policies that pertain to the web application development recommendations of the report. OIS will assess the policies and provide updates as appropriate. OIS will also explore the development of new policies, standards, or memoranda as needed.
 - Policy for Software Development Secure Coding Practices (draft is in clearance process),
 - Security and Privacy Language for Information and Information Technology Procurements
2. OIS will work with designated acquisition points of contact to ensure that procurement provisions regarding security standards are appropriately incorporated into application development contracts.

OIG Recommendation 4 –

(b)(7)F

(b)(7)F

Office of Management and Budget A-123 reviews, follow-up testing for Plan of Action and Milestones, and other mechanisms that are in place to monitor and test for internal cybersecurity vulnerabilities.

OIS Actions –

1. OIS, in collaboration with the relevant divisions within the OCIO, has identified the following existing policies pertaining to the recommendations of the report, and will consider updates to reflect the recommendations to test for (b)(7)F
 - HHS Information Security and Privacy Policy (IS2P),
 - Addendum to the HHS Information Systems Security and Privacy Policy (IS2P),



OFFICE OF THE CHIEF INFORMATION OFFICER

DEPARTMENT OF HEALTH AND HUMAN SERVICES

- HHS Plan of Action and Milestones (POA&M) Standard (draft is in clearance process),
 - HHS Policy for Patch and Vulnerability Management (draft is in clearance process)
2. OIS will work with each OpDiv to ensure that they implement tests (b)(7)F and continuously monitor applications. Any findings will be documented, reported, and remediated consistent with the HHS POA&M requirements. Per these requirements, OpDivs will be required to identify remediation activities, timeframes, and resources required to address audit findings. OIS will review progress on a regular basis through review of POA&Ms.

Through the HHS-wide CISO and CIO Councils, OIS will ensure OpDivs remain engaged on enacting these recommendations. OIS appreciates the continuing partnership with the OIG. Audit activities, such as those conducted in the *General Penetration Testing of HHS OpDivs*, help us better understand risks and vulnerabilities in our information systems and cybersecurity policies, and enable OIS to undertake specific, targeted activities to better protect the information with which HHS is entrusted.