Department of Health and Human Services

OFFICE OF INSPECTOR GENERAL

THE CENTERS FOR MEDICARE & MEDICAID SERVICES HAD POLICIES AND PROCEDURES IN PLACE TO MITIGATE VULNERABILITIES IN A TIMELY MANNER, BUT IMPROVEMENTS ARE NEEDED

Inquiries about this report may be addressed to the Office of Public Affairs at Public.Affairs@oig.hhs.gov.

Amy J. Frontz
Deputy Inspector General
for Audit Services

June 2022
A-18-20-06500

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 audits 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 IS AVAILABLE TO THE PUBLIC
at https://oig.hhs.gov

Section 8M of the Inspector General Act, 5 U.S.C. App., requires that OIG post its publicly available reports on the OIG website.

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: June 2022
Report No. A-18-20-06500

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

The Centers for Medicare & Medicaid Services Had Policies and Procedures in Place To Mitigate Vulnerabilities in a Timely Manner, but Improvements Are Needed

Why OIG Did This Audit

Effective April 29, 2019, the Department of Homeland Security's Binding Operational Directive 19-02 (BOD 19-02) requires Federal agencies to remediate known "critical" vulnerabilities within 15 days of discovery and "high" vulnerabilities within 30 days of discovery. We have identified through previous oversight work that the Department of Health and Human Services has not always complied with BOD 19-02.

The cybersecurity community has adopted use of the Common Vulnerabilities and Exposure (CVE) list, which provides public information about vulnerabilities and the ways that they can be exploited. Malicious actors can research the CVE list and tailor attacks to systems that may be vulnerable if a security patch or update has not been implemented.

Our objective was to determine whether CMS had controls in place to remediate known cybersecurity vulnerabilities in accordance with Federal regulations.

How OIG Did This Audit

We reviewed CMS's policies and procedures for flaw remediation, interviewed CMS officials, and reviewed system security plans to determine whether CMS's flaw remediation controls were adequate.

What OIG Found

CMS had controls in place to remediate known vulnerabilities in accordance with Federal regulations and standards; however, it did not consistently apply security updates to systems with known vulnerabilities and did not consistently upgrade or patch operating systems that had reached the end of life period and were no longer supported by the vendor. This occurred because CMS did not have effective management oversight to ensure that CMS mitigated vulnerabilities in a timely manner. As a result, some CMS systems had open vulnerabilities that were vulnerable to exploitation by malicious actors beyond the acceptable limits defined in the BOD.

What OIG Recommends and CMS' Comments

We recommend that CMS: (1) remediate the vulnerabilities identified on internet-facing systems and implement procedures to ensure compliance with BOD 19-02 requirements; (2) implement procedures to ensure that unsupported software that no longer receives security updates, repairs, bug fixes, and threat mitigation is replaced prior to the known EOS or implement compensating controls (if possible) and accept risk in accordance with existing CMS policies and procedures; (3) implement oversight to ensure corrective actions are performed in accordance with Federal requirements and in the timeframe set forth in CMS policy; and (4) implement a process to centralize the monitoring and reporting of vulnerabilities identified in all CMS systems across all CMS data centers.

CMS concurred with all our recommendations and provided supporting documentation to remediate the technical vulnerabilities identified.

TABLE OF CONTENTS

INTRODUCTION

WHY WE DID THIS AUDIT

Federal requirements mandate that Federal agencies review and remediate vulnerabilities on internet-facing systems identified by the National Cybersecurity and Communications Integration Center (NCCIC). Effective April 29, 2019, the Department of Homeland Security's (DHS's) Binding Operational Directive 19-02 (BOD 19-02) requires Federal agencies to remediate known "critical" vulnerabilities within 15 days of discovery and "high" vulnerabilities within 30 days of discovery.

The cybersecurity community has adopted use of the Common Vulnerabilities and Exposure (CVE) list. The mission of the CVE Program is to identify, define, and catalog publicly disclosed cybersecurity vulnerabilities. There is one CVE Record for each vulnerability in the catalog. Information technology (IT) and cybersecurity professionals use CVE Records to ensure they are discussing the same issue, and to coordinate their efforts to prioritize and address the vulnerabilities. Conversely, some malicious actors research the CVE list and use the information to tailor attacks against systems that may be vulnerable if a security patch or update has not been implemented. For example, malicious actors used a vulnerability identified in the CVE list to target a system to infect it with a malware application called "LOKI" that stole usernames and passwords. This malware remained active for over 3 years, and in September 2020 the U.S. Cybersecurity and Infrastructure Agency (CISA) issued an updated notification.

In fiscal year (FY) 2020, more than 145 million Americans relied on the programs that the Department of Health and Human Services (HHS), Centers for Medicare & Medicaid Services (CMS) administers.[1] These CMS programs depend on the confidentiality, integrity, and availability of IT systems and the data they contain. Therefore, we conducted this audit to assess CMS's controls for ensuring that known cybersecurity vulnerabilities are remediated within federally required timeframes.

OBJECTIVE

Our objective was to determine whether CMS had controls in place to remediate known cybersecurity vulnerabilities in accordance with Federal regulations.

[1] HHS, CMS, fiscal year 2020, *Justification of Estimates for Appropriations Committees*.

BACKGROUND

CMS Programs

CMS operates and oversees the two largest Federal health care programs—Medicare and Medicaid—as well as the Children's Health Insurance Program (commonly known as CHIP). These three programs provide health care insurance for one in four Americans. According to the CMS annual financial report, CMS outlays for these programs were approximately $1,255 billion in FY 2020, which was approximately 19 percent of total Federal Government spending.

CMS has hundreds of systems across dozens of data centers to support its mission. CMS uses automated vulnerability management tools to identify vulnerabilities. To help ensure the timely mitigation of known vulnerabilities, the 2017 CMS Acceptable Risk Safeguards (ARS) defines timeframes for remediation.

Flaw Identification and Remediation

Flaw identification and remediation for Federal agencies generally consists of a four-step process—identification, research, remediation, and closure. According to the National Institute of Standards and Technology (NIST), Federal agencies are tasked with identifying information systems affected or potentially affected by announced security flaws, including potential vulnerabilities resulting from those flaws.[2] Identification of a flaw can come from numerous sources such as DHS's CISA and NCCIC, internal vulnerability scans, or vendor supplied information. Once a flaw has been identified, the system owners research the flaw to determine the critically level for the system. If the flaw requires remediation, the system owners take the required actions to remediate the flaw. CISA has defined timeframes by which agencies must remediate certain flaws. The BOD 19-02, issued by CISA, requires that critical flaws in internet-facing systems be remediated within 15 days of discovery, and those flaws deemed as a high should be addressed within 30 days. Further, NIST Special Publication 800-53, Revision 4, security control SI-2 requires that agencies install security relevant software and firmware updates within a timeframe established by the agency. The agency should run a vulnerability scan after it takes action to address the flaw to confirm that it no longer exists and consider the flaw remediated.

In 1999, the United States' National Cybersecurity Federally Funded Research and Development Center, operated by the Mitre Corporation, launched the CVE system. The system supports the CVE Program and provides a reference method for publicly known information-security vulnerabilities and exposures. The mission of the CVE Program is to identify, define, and catalog publicly disclosed cybersecurity vulnerabilities. There is one CVE Record for each vulnerability in the catalog. The vulnerabilities are discovered, assigned, and published by organizations from around the world that have partnered with the CVE Program. Partners

[2] NIST SP 800-53, Revision 4, SI-2, Flaw Remediation, Supplemental Guidance.

publish CVE Records to communicate consistent descriptions of vulnerabilities. IT and cybersecurity professionals use CVE Records to ensure they are discussing the same issue, and to coordinate their efforts to prioritize and address the vulnerabilities.[3] Use of the CVE Program by U.S. agencies was recommended by NIST in the NIST Special Publication 800-51, "Use of the CVE Vulnerability Naming Scheme."[4]

A vendor may stop providing support for its product, often referred to as End-of-Life (EOL). Typically, this means that the vendor will not provide security updates or patches for vulnerabilities that are discovered after the support stops. The client becomes responsible for remediating any vulnerabilities discovered after the vendor support ends. A vulnerability in a product that is not remediated remains open to exploitation and places the system using the product at risk.

HOW WE CONDUCTED THIS AUDIT

We reviewed CMS's policies and procedures for flaw remediation, interviewed CMS officials, and reviewed system security plans to determine whether CMS's flaw remediation controls were adequate. Our testing methodology assessed whether CMS implemented its flaw remediation process, as described in its System Security and Privacy Plan (IS2P2), in a timely manner and in accordance with the ARS and BOD 19-02. We communicated to CMS our preliminary findings in advance of issuing our draft report.

We conducted this performance audit 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 objectives.

Appendix A describes our audit scope and methodology, and Appendix B contains Federal requirements and CMS guidance for flaw remediation.

FINDINGS

CMS had controls in place to remediate known vulnerabilities in accordance with Federal regulations and standards; however, it did not consistently apply security updates to systems with known vulnerabilities and did not consistently upgrade or patch operating systems. This occurred because CMS had oversight gaps that resulted in a failure to ensure that it mitigated vulnerabilities in accordance with the timeframes established in BOD 19-02. As a result, some CMS systems had vulnerabilities beyond the acceptable limits defined in the BOD 19-02.

[3] Available online at https://www.cve.org/About/Overview. Accessed on Mar. 24, 2022.

[4] Available online at https://www.cve.org/About/History. Accessed on Mar. 24, 2022.

CMS DID NOT FULLY COMPLY WITH EXECUTIVE ORDER BOD 19-02

BOD 19-02 requires Federal agencies to remediate critical and high vulnerabilities on their internet-facing systems.[5] Remediation must occur within 15 days of the detection of a "critical" vulnerability and within 30 days of the detection of a "high" vulnerability. According to BOD 19-02, the Federal Government and its industry partners indicate that the average time it takes to exploit a vulnerability after it has been discovered is decreasing as malicious actors have become more skilled, persistent, and knowledgeable about software updates, security advisories, threat bulletins, and patches.[6] Industry reports estimated that malicious actors are now able to exploit a vulnerability within 15 days (on average) of discovery. The likelihood of a cyberattacker (e.g., State-sponsored attackers, cybercriminals, insiders, hacktivists, etc.) exploiting a vulnerability increases as time elapses between vulnerability detection and remediation.

We determined that two vulnerabilities were not remediated within 30 days as required. The vulnerabilities in the systems remained unpatched after CISA's Cyber Hygiene service had identified and reported them to CMS.[7] CMS officials said on September 10, 2021, that they had investigated and remediated the two vulnerabilities. However, they did not provide us with supporting documentation, such as change logs or software update logs, that validated the vulnerabilities had been remediated.

CMS was not in full compliance with the Federal requirement because of oversight gaps. Specifically, dashboards and metrics used to monitor and report on vulnerabilities did not fully capture vulnerability information.

CMS DID NOT APPLY SECURITY PATCHES TO ALL SYSTEMS WITH KNOWN VULNERABILITIES

Federal regulations as well as HHS and CMS policies require the timely mitigation of vulnerabilities, typically through the application of patches (also known as hot fixes or service packs).[8]

CMS did not apply some security updates to systems with known vulnerabilities in a timely manner. We identified vulnerabilities with a CVE severity rating of "moderate" that had not

[5] The risk level of each vulnerability is assigned in the Weekly Cyber Hygiene by the National Cybersecurity and Communications Integration Center.

[6] Available online at https://cyber.dhs.gov/bod/19-02/. Accessed on Dec. 14, 2021.

[7] CISA performs regular network and vulnerability scans of Federal agencies internet-facing systems under authority of Title XXII of the Homeland Security Act (6 U.S.C. § 651) and delivers a weekly report for action.

[8] NIST 800-53, Revision 4, System and Information Integrity, HHS Information Security and Privacy Policy, CMS Acceptable Risk Safeguards.

been mitigated.[9] According to an industry report, malicious actors tend to exploit as many older, known vulnerabilities as they can simultaneously.[10] We also identified reported vulnerabilities with a severity rating of low.[11] Installing timely patches would have remediated most of the vulnerabilities.

CMS did not properly follow procedures to address known vulnerabilities in a timely manner in compliance with Federal requirements. Because CMS did not patch known vulnerabilities within the required timeframe, cyberattackers could have exploited the vulnerabilities.

CMS DID NOT PATCH OR UPGRADE ALL OPERATING SYSTEMS THAT ARE NO LONGER VENDOR SUPPORTED

Federal standards and HHS policy require that organizations (such as CMS) either replace system components that are no longer available from the developer or document a designated official's approval for the continued use of unsupported systems.[12] Software that has reached the end of support (EOS) and no longer receives security updates or patches from the vendor could be exploited.

Using software that has known vulnerabilities and no longer receives patches from the vendor because the EOS period has expired increases the risk of exploitation by cyberattackers. Research has shown that the Microsoft family of software is the most frequently impacted by vulnerabilities (Figure 2 on the next page).

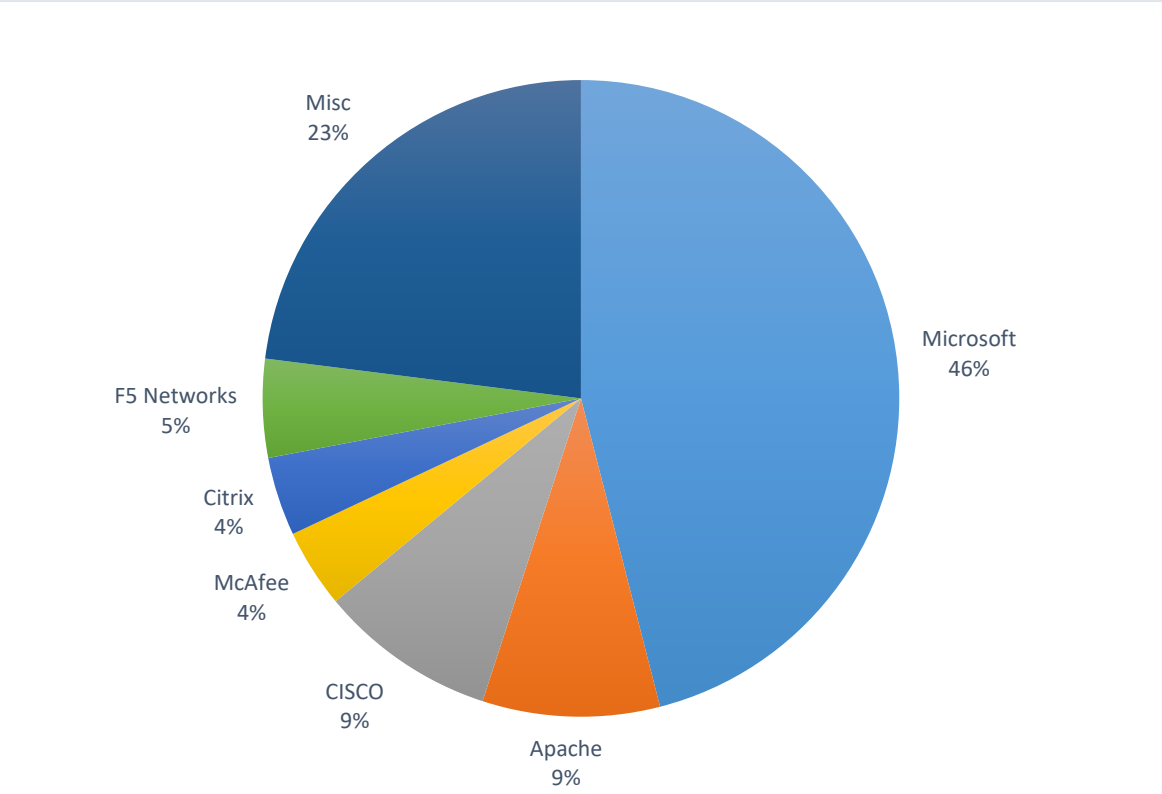
[9] Moderate or medium severity have a CVE base score of 4.0 to 6.9.

[10] Verizon's *2021 Data Breach Investigations Report.* Available online at https://www.verizon.com/business/resources/reports/dbir/. Accessed on Feb. 24, 2022.

[11] Low can be defined by the agency's rules in the scanning tools or the CVE baseline score.

[12] HHS Information Systems Security and Privacy Policy 2014, section 4.1.3, states that information assurance conducted within the department must be consistent with guidance, methodologies, and intent prescribed by the NIST SP series, in particular NIST SP 800-53.

Figure 2: Vendors Impacted by Third Quarter Top 2020 Vulnerabilities*



* Insikt Group analysis of 2020 Q3 NVD data.

Vendors typically support products for specific time periods.[13] This support is considered mainstream and includes security updates and application enhancements. After the time period, products may transition to an extended service period. During the extended service period, vendors issue security updates free of charge and offer fee-based support plans. Once the extended service period ends, vendors no longer supply security updates or support. Unpatched products being used after the support ends are more vulnerable to attacks. We sampled hosts across CMS data centers and determined that some were past mainstream support. In a few instances, CMS did not provide documents that demonstrated extended service contracts had been purchased.

CMS issued Plans of Action and Milestones (POA&Ms) for software that was past EOS. A POA&M identifies an issue that needs to be addressed and the steps needed to address the issue. The POA&M also provides estimated milestones for completing the steps and used to track updates to the work performed. POA&Ms undergo multiple levels of review prior to closure and are tracked by CMS. CMS did not take action to address vulnerabilities identified in the POA&M. CMS's POA&M process allowed some unsupported operating systems to remain active on the network.

[13] Microsoft Lifecycle Policy offers 5 years of mainstream support. Microsoft no longer publishes updates or security updates for that product after 5 years.

RECOMMENDATIONS

To improve its cybersecurity posture, we recommend that the Centers for Medicare & Medicaid Services:

- remediate the vulnerabilities identified and implement procedures to ensure compliance with BOD 19-02 requirements,

- implement procedures to ensure the replacement of unsupported software prior to the known EOS or implement compensating controls (if possible) and accept risks in accordance with existing CMS policies and procedures,

- implement oversight to ensure corrective actions are performed in accordance with Federal requirements and in the timeframe set forth in CMS policy, and

- implement a process to centralize the monitoring and reporting of vulnerabilities identified in all CMS systems across all CMS data centers.

CMS COMMENTS AND OFFICE OF INSPECTOR GENERAL RESPONSE

In written comments, CMS stated that it concurred with all our recommendations. Regarding our first recommendation, CMS stated that it has remediated the two identified vulnerabilities and implemented procedures to ensure compliance with BOD 19-02 requirements and provided documentation to support this statement. For the remaining recommendations, CMS described the steps it has taken or is planning to take to implement the procedural recommendations. CMS's comments are included in their entirety as Appendix C.

We are encouraged that CMS has taken steps to remediate the vulnerabilities identified in this report and is working to implement our remaining recommendations, which should serve to protect CMS systems and sensitive information therein, supporting its mission essential functions.

APPENDIX A: AUDIT SCOPE AND METHODOLOGY

SCOPE

We audited CMS's compliance with Federal requirements and internal controls over flaw remediation. We reviewed CMS's flaw remediation process, policies, and procedures for patching or mitigating the risk of vulnerabilities that affect CMS information systems.

We conducted our audit work from October 2020 through April 2022.

METHODOLOGY

To accomplish our objective, we assessed whether CMS had implemented flaw remediation for information systems in accordance with Federal regulations and guidance for vulnerability identification, patch management, and remediation. We examined data centers' review and remediation of known vulnerabilities. We reviewed CMS's policies and procedures, interviewed staff, and reviewed system security documentation to determine whether CMS flaw remediation controls were adequate.

We conducted this performance audit 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 objectives.

APPENDIX B: FEDERAL REQUIREMENTS AND GUIDANCE

FEDERAL REQUIREMENTS

Section 3554 of the Federal Information Security Modernization Act (FISMA) of 2014 (P.L. 113–283) directs agencies to comply with the policies, procedures, standards, and guidelines promulgated under section 11331 of Title 40, which requires that Federal information systems meet the minimum information security system requirements described under section 20(b) of the National Institute of Standards and Technology Act (15 U.S.C. 278g-3).

Federal Information Processing Standards (FIPS) Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, is a mandatory Federal standard developed by NIST in response to FISMA. To comply with the Federal standard, organizations:

(i) determine the security category of their information system in accordance with FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*;

(ii) derive the information system impact level from the security category in accordance with FIPS 200; and

(iii) apply the appropriately tailored set of baseline security controls in NIST Special Publication 800-53, R4*, Security and Privacy Controls for Federal Information Systems and Organizations*.

Organizations have flexibility in applying the baseline security controls in accordance with the guidance provided in NIST SP 800-53, Revision 4. This flexibility allows an organization to tailor its security control baseline so that it more closely aligns with the organization's mission and business requirements and its environment of operation.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY REQUIREMENTS

NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets in furtherance of NIST's statutory responsibilities under FISMA (P.L. 107–347). The NIST guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*, section 8b (3), "Securing Agency Information Systems." NIST states the following:

> While agencies are required to follow NIST guidance in accordance with OMB policy, there is flexibility within NIST's guidance in how agencies apply the

> guidance. When assessing federal agency compliance with NIST guidance, auditors, evaluators, and assessors should consider the intent of the security concepts and principles articulated within the particular guidance document and how the agency applied the guidance in the context of its specific mission responsibilities operational environments, and unique organizational conditions.[14]

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

Section 3.19, System and Information Integrity SI-2, states:

> Organizations identify information systems affected by announced software flaws including potential vulnerabilities resulting from those flaws and report this information to designated organizational personnel with information security responsibilities. Security-relevant software updates include, for example, patches, service packs, hot fixes, and anti-virus signatures

Section 3.19, System and Information Integrity SI-2, has four control areas:

1. identify, report, and correct system flaws;
2. test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;
3. install security-relevant software and firmware updates within [Assignment: organization defined time period] of the release of the updates; and
4. incorporate flaw remediation into the organizational configuration management process.

[14] NIST SP 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems, Page iv.*

SI-2 also provides the following control enhancements:

(1) FLAW REMEDIATION | CENTRAL MANAGEMENT [Withdrawn: Incorporated into PL-9.]

(2) FLAW REMEDIATION | AUTOMATED FLAW REMEDIATION STATUS Determine if system components have applicable security-relevant software and firmware updates installed using [Assignment: organization-defined automated mechanisms] [Assignment: organization-defined frequency]. Discussion: Automated mechanisms can track and determine the status of known flaws for system components. Related Controls: CA-7, SI-4.

(3) FLAW REMEDIATION | TIME TO REMEDIATE FLAWS AND BENCHMARKS FOR CORRECTIVE ACTIONS (a) Measure the time between flaw identification and flaw remediation; and (b) Establish the following benchmarks for taking corrective actions: [Assignment: organization-defined benchmarks]. Discussion: Organizations determine the time it takes on average to correct system flaws after such flaws have been identified and subsequently establish organizational benchmarks (i.e., timeframes) for taking corrective actions. Benchmarks can be established by the type of flaw or the severity of the potential vulnerability if the flaw can be exploited. Related Controls: None.

(4) FLAW REMEDIATION | AUTOMATED PATCH MANAGEMENT TOOLS Employ automated patch management tools to facilitate flaw remediation to the following system components: [Assignment: organization-defined system components]. Discussion: Using automated tools to support patch management helps to ensure the timeliness and completeness of system patching operations. Related Controls: None.

(5) FLAW REMEDIATION | AUTOMATIC SOFTWARE AND FIRMWARE UPDATES Install [Assignment: organization-defined security-relevant software and firmware updates] automatically to [Assignment: organization-defined system components]. Discussion: Due to system integrity and availability concerns, organizations consider the methodology used to carry out automatic updates. Organizations balance the need to ensure that the updates are installed as soon as possible with the need to maintain configuration management and control with any mission or operational impacts that automatic updates might impose. Related Controls: None.

(6) FLAW REMEDIATION | REMOVAL OF PREVIOUS VERSIONS OF SOFTWARE AND FIRMWARE Remove previous versions of [Assignment: organization-defined software and firmware components] after updated versions have been installed. Discussion: Previous versions of software or firmware components that are not removed from the system after updates have been installed may be exploited by adversaries. Some products may automatically remove previous versions of software and firmware from

the system. Related Controls: None

NIST SP 800-53, Revision 4, section 3.12, Planning PL-9 Central Management, states:

> Central management refers to the organization-wide management and implementation of selected security controls and related processes. Central management includes planning, implementing, assessing, authorizing, and monitoring the organization-defined, centrally managed security controls and processes. As central management of security controls is generally associated with common controls, such management promotes and facilitates standardization of security control implementations and management and judicious use of organizational resources. Centrally managed security controls and processes may also meet independence requirements for assessments in support of initial and ongoing authorizations to operate as part of organizational continuous monitoring.

NIST SP 800-53, Revision 4, section 3.12, Unsupported System Components, states:

> The organization replaces information system components when support for the components is no longer available from the developer, vendor, or manufacturer and provide justification and documents approval for the continued use of unsupported system components required to satisfy mission/business needs.

U.S. DEPARTMENT OF HOMELAND SECURITY BINDING OPERATIONAL DIRECTIVE 19-02, *Critical Vulnerability Mitigation Requirement for Federal Civilian Executive Branch Departments and Agencies' Internet-Accessible Systems*

Binding Operational Directive 19-02 established requirements for Federal agencies to review and remediate critical vulnerabilities on internet-facing systems identified by the NCCIC within 30 days of issuance of their weekly Cyber Hygiene report.

CMS ACCEPTABLE RISK SAFEGUARDS 3.1

The *Centers for Medicare & Medicaid Services Information Security and Privacy Acceptable Risk Safeguards* provides guidance to CMS and its contractors about the minimum acceptable level of security controls (i.e., the minimum security and privacy control baselines,[15] collectively known as the CMS Minimum Security Requirement (CMSR) baselines) that must be implemented by CMS and CMS contractors to protect CMS's information and information systems, including CMS Sensitive Information. The CMSR is based on:

[15] A control baseline is the minimum list of security controls required for safeguarding an IT system based on the organizationally identified needs for confidentiality, integrity, and/or availability. A different baseline exists for each security category defined by NIST FIPS 199, "Standards for Security Categorization of Federal Information and Information Systems."

- NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, dated April 2013;

- Federal Risk and Authorization Management Program;

- HHS *Information Systems Security and Privacy Policy (IS2P);*

- *CMS Information Systems Security and Privacy Policy (CMS IS2P2) CMS-CIO-POL-SEC-2016-0001;*

- CMS policies, procedures, and guidance;

- Other Federal and non-Federal guidance resources; and

- Industry leading information security and privacy practices adopted by CMS.

APPENDIX C: CENTERS FOR MEDICARE & MEDICAID SERVICES COMMENTS

DEPARTMENT OF HEALTH & HUMAN SERVICES

Centers for Medicare & Medicaid Services

Administrator
Washington, DC 20201

DATE: May 31, 2022

TO: Amy J. Frontz
Deputy Inspector General for Audit Services
Office of Inspector General

FROM: Chiquita Brooks-LaSure
Administrator
Centers for Medicare & Medicaid Services

SUBJECT: Office of Inspector General (OIG) Draft Report: The Centers for Medicare & Medicaid Services Had Policies and Procedures in Place To Mitigate Vulnerabilities in a Timely Manner, but Improvements Are Needed (A-18-20-06500)

The Centers for Medicare & Medicaid Services (CMS) appreciates the opportunity to review and comment on the Office of Inspector General's (OIG) draft report.

The security of CMS systems and beneficiary health data is a top priority for CMS. To secure against potential vulnerabilities, CMS vigilantly monitors, tests, and strengthens its systems against cyber-attacks and has procedures and processes in place to quickly identify, mitigate, and remove threats, in accordance with the Federal Information Security Modernization Act of 2014 (FISMA) requirements and guidelines issued by the Cybersecurity & Infrastructure Security Agency (CISA).

As noted in the OIG's findings, CMS has controls in place to remediate known vulnerabilities in accordance with Federal regulations and standards. CMS policies and procedures include requirements for the identification, reporting, and correction of information system flaws in line with Binding Operational Directive 19-02 (BOD 19-02), Vulnerability Remediation Requirements for Internet Accessible Systems. BOD 19-02 requires Federal agencies to remediate known "critical" vulnerabilities within 15 days of discovery and "high" vulnerabilities within 30 days of discovery. CMS uses cyber hygiene scans provided by CISA to enhance CMS's overall vulnerability management efforts.

Since 2015, CMS has participated in CISA's Continuous Diagnostics and Mitigation (CDM) program, which is a dynamic approach to fortifying the cybersecurity of government networks and systems. CDM provides federal departments and agencies with capabilities and tools that identify cybersecurity risks on an ongoing basis, prioritizes these risks based upon potential impacts, and enables cybersecurity personnel to mitigate the most significant problems first. CMS continues to improve the overall security posture of the environment and enhance the tools used to monitor for vulnerabilities in CMS systems and datacenters.

OIG's recommendations and CMS's responses are below.

OIG Recommendation
The OIG recommends that CMS remediate the vulnerabilities identified and implement procedures to ensure compliance with BOD 19-02 requirements.

CMS Response
CMS concurs with this recommendation. CMS has remediated the two identified vulnerabilities. CMS continues to use cyber hygiene scans provided by CISA to enhance CMS's overall vulnerability management efforts.

OIG Recommendation
The OIG recommends that CMS implement procedures to ensure the replacement of unsupported software prior to the known EOS or implement compensating controls (if possible) and accept risks in accordance with existing CMS policies and procedures.

CMS Response
CMS concurs with this recommendation. CMS has removed or replaced all unsupported software identified by the OIG. CMS regularly monitors the status of decommissioning and replacing end of life software. CMS issues Plans of Action and Milestones (POA&Ms) for software that is past end of service to track known issues and document planned steps to address the issue. CMS is working to implement procedures to ensure the replacement of unsupported software prior to the known end of service date.

OIG Recommendation
The OIG recommends that CMS implement oversight to ensure corrective actions are performed in accordance with Federal requirements and in the timeframe set forth in CMS policy.

CMS Response
CMS concurs with this recommendation. CMS has remediated the "moderate" vulnerabilities OIG identified. CMS has improved oversight of vulnerabilities at all severity levels and is assessing how to better ensure corrective actions for lower level vulnerabilities are taken in the timeframes set forth in CMS policy.

OIG Recommendation
The OIG recommends that CMS implement a process to centralize the monitoring and reporting of vulnerabilities identified in all CMS systems across all CMS data centers.

CMS Response
CMS concurs with this recommendation. As part of the Cybersecurity & Infrastructure Security Agency Continuous Diagnostics and Mitigation program, CMS has centralized visibility into the monitoring and reporting of vulnerabilities identified at all CMS systems and data centers. CMS continues to improve the overall security posture of the environment and enhance the tools used to monitor for vulnerabilities.