OFFICE OF INSPECTOR GENERAL

U.S. Department of Energy

AUDIT REPORT

DOE-OIG-17-08 September 2017

THE DEPARTMENT OF ENERGY'S IMPLEMENTATION OF MULTIFACTOR AUTHENTICATION CAPABILITIES

Department of Energy
Washington, DC 20585

September 21, 2017

MEMORANDUM FOR THE SECRETARY

April Stephenson

FROM: April Stephenson
Acting Inspector General

SUBJECT: INFORMATION: Audit Report on "The Department of Energy's Implementation of Multifactor Authentication Capabilities"

BACKGROUND

The Department of Energy operates many types of information systems supporting mission related activities such as nuclear security, scientific research and development, and environmental management. Strengthening cybersecurity over its information technology environment is a significant challenge facing the Department. Federal requirements and industry best practices indicate that multifactor authentication is one of the most effective methods of safeguarding information systems. In its most basic form, authentication is the process of verifying the identity of a user prior to allowing access to an information system. While the most common method of authentication is username and password, multifactor authentication adds rigor to the authentication process using two or more different authenticators such as hardware security tokens and personal identity verification (PIV) cards.

Federal requirements concerning multifactor authentication on Federal information systems, including those operated by contractors, have existed for many years. For instance, the Office of Management and Budget (OMB) issued M-05-24, *Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors*, in August 2005 which required Federal agencies to implement multifactor authentication, in the form of PIV cards, for logical and physical access to Federal facilities and information systems. More recently, in June 2015, OMB initiated a 30-day Cybersecurity Sprint initiative to further emphasize access controls over Federal information systems by directing that all privileged users and most standard users utilize PIV card credentials to access information systems by September 30, 2016. We initiated this audit to determine whether the Department effectively implemented multifactor authentication when securing its information systems.

RESULTS OF AUDIT

The Department made progress towards fully implementing multifactor authentication in accordance with Federal requirements. Specifically, the Department recently invigorated its efforts to meet the demands of the OMB Cybersecurity Sprint; however, we found that additional effort was needed for access to technology resources to ensure that multifactor authentication, including the use of PIV cards, was fully implemented across the Department. In particular, our review of 18 Federal information systems, including those systems operated by contractors, identified weaknesses related to ensuring adequate protections over access to network and application resources, and noted that information reported to OMB related to the Cybersecurity Sprint was not always consistent. Specifically, we found:

- Although requirements existed for more than 10 years, none of the locations reviewed had fully implemented multifactor authentication for secure access to information systems and resources. In particular, we found that the sites reviewed had not always implemented applicable requirements such as the use of PIV cards for authenticating privileged or standard users, as appropriate. Privileged users typically maintain elevated functions such as security and network management, while a standard user does not have elevated privileges above those typically required for the daily performance of their duties. Although some sites only required users to input a username and password to obtain access to their networks when in the office, stronger multifactor authentication such as PIV credentials were not implemented. In addition, while all sites permitted remote access to network resources using various forms of multifactor authentication, sites had not adequately identified and assessed the risks related to remote access to determine whether controls were appropriate.

- Federal and contractor locations tested had not always considered the applicability of multifactor authentication for software applications, including those that contained sensitive information such as personally identifiable information and personal health information. While we recognize that not all applications will require multifactor authentication for access, we noted that only one of the locations reviewed used multifactor authentication to access software applications. According to National Institute of Standards and Technology Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, organizations should employ risk-based identification and authentication mechanisms at the application level, when necessary, to provide increased information security.

- Information reported to OMB by the Department related to progress implementing the Cybersecurity Sprint was not consistent and did not portray an accurate accounting of its use of multifactor authentication. For instance, while some locations reported their results based on the number of users, others reported on the number of accounts. In addition, contrary to the intent of the Cybersecurity Sprint, we noted that the Department established several exception categories to OMB requirements which resulted in thousands of exceptions for Federal and/or contractor users. Department officials stated that they had coordinated with OMB regarding the exception process; however, they were unable to provide documentation to support their assertion. Although the Department began reporting exceptions in September 2016, we found that it was difficult to accurately gauge the Department's overall progress in meeting OMB requirements.

The weaknesses identified occurred, in part, because officials had not fully planned for implementation of multifactor authentication on information systems. Department guidance and requirements related to multifactor authentication technologies also were not always communicated effectively. In particular, even though Federal requirements related to the use of multifactor authentication, including PIV cards, had existed for many years, we noted that the Department had not fully deployed its enterprise-wide identity, credential, and access management program to address multifactor authentication. Furthermore, the Department had yet to officially approve its multifactor authentication implementation plan in response to the OMB Cybersecurity Sprint. Although management indicated that the implementation plan was a living document, we noted that approval of the plan was not formally documented. In addition, contractor representatives at certain locations stated that some multifactor authentication requirements were not implemented because requirements were not specifically included in site-level contracts. Contractor representatives added that multifactor authentication implementation by the OMB deadline would be difficult because of a lack of adequate funding and technical direction. We also found that a lack of effective communication and misinterpretation within the Department regarding the defined Cybersecurity Sprint reporting criteria resulted in instances of inconsistent reporting to OMB. To help address this issue, Office of the Chief Information Officer officials reported that quality assurance steps were put in place to cross-check information provided by the entities to potentially minimize such reporting errors.

Without development and implementation of a Department-wide multifactor authentication process, the Department's information, including sensitive data, will continue to be at a higher-than-necessary risk of compromise. In addition, the Department will risk potentially duplicating efforts and encountering additional delays unless it adequately considers and identifies implementation specifics such as budget priorities, exceptions, and enterprise provided services. Furthermore, officials will continue to struggle with fully understanding the Department's operating environment and will be unable to provide an accurate representation of its environment unless reporting criteria is fully communicated and understood by all entities. Based on the Department's progress at the time of our review, officials faced significant challenges related to meeting OMB's goals of ensuring that all privileged users and 85 percent of standard users use PIV credentials. As a result of those challenges, the Department reported it had implemented PIV cards for approximately 82 percent of privileged users and 52 percent of standard users as of September 2016. While a significant improvement given the Department's environment, the results were still well below the OMB requirements.

Notably, the Department had made progress towards implementing multifactor authentication. For instance, the Department reported that it had made significant progress subsequent to our test work to increase the number of users utilizing multifactor authentication to access information systems. The Department also reported that it had conducted a number of training sessions and made available various resources to help programs and sites meet multifactor authentication requirements. We have made recommendations that, if fully implemented, should help the Department enhance its cybersecurity posture through effective implementation of multifactor authentication.

MANAGEMENT RESPONSE

Management concurred with the report's recommendations and indicated that corrective actions had been initiated or were planned to address the issues identified in the report. Management's comments and our responses are summarized in the body of the report. Management's formal comments are included in Appendix 4.

Attachment

cc: Deputy Secretary
Chief of Staff
Administrator for the National Nuclear Security Administration
Acting Under Secretary for Science and Energy
Acting Under Secretary for Management and Performance
Chief Information Officer
Acting Chief Financial Officer

THE DEPARTMENT OF ENERGY'S IMPLEMENTATION OF MULTIFACTOR AUTHENTICATION

TABLE OF CONTENTS

Audit Report

Details of Finding 1

Recommendations..11

Management Response and Auditor Comments...12

Appendices

1. Objective, Scope, and Methodology...13
2. Related Criteria 15
3. Prior Reports 16
4. Management Comments 18

THE DEPARTMENT OF ENERGY’S IMPLEMENTATION OF MULTIFACTOR AUTHENTICATION

DETAILS OF FINDING

As defined by the National Institute of Standards and Technology, multifactor authentication requires the use of two or more factors to achieve authentication, including something you know, something you have, and/or something you are. Federal requirements and industry best practices indicate that multifactor authentication is one of the most effective methods of safeguarding information systems. In its most basic form, authentication is the process of verifying the identity of a user, process, or device prior to allowing access to an information system. While the most common method of authentication is username and password, multifactor authentication adds rigor to the authentication process by using two or more different factors. Commonly utilized factors include biometrics and hardware security tokens. Personal identity verification (PIV) cards, which can be considered a type of token and is the Federal standard for physical and logical access to Federally controlled facilities and information systems set by the Office of Management and Budget (OMB), are also used. PIV cards, are secure, smart card identification credentials that use an embedded microchip to verify the identity and access privileges of the user. They include identity information of the individual to whom the card is issued, as well as graduated criteria for assuring the identity of the user based on the environment and desired confidence. PIV cards are the OMB mandated standard for achieving multifactor authentication.

Figure 1: Example of PIV Card

OMB M-05-24, *Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors* (August 2005), required Federal agencies to implement the HSPD-12 PIV card as the standard for a secure and reliable form of controlling logical and physical access to Federal facilities and information systems, including local and network systems operated by Federal and contractor employees. Lagging progress by agencies related to implementing PIV cards resulted in the issuance of OMB M-11-11, *Continued Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors*, in February 2011. The updated guidance required that each agency develop and issue an implementation policy by April 2011 that required the use of the PIV credentials as the common means of authentication for access to facilities, networks, and information systems by the beginning of fiscal year 2012[1].

In April 2015, the Office of Personnel Management identified a data breach impacting more than 21 million individuals and highlighted cybersecurity challenges and concerns across the Federal government, including the need to enhance the use of multifactor authentication. As a result, in June 2015, the United States Chief Information Officer, in coordination with OMB, launched a 30-day Cybersecurity Sprint to improve cybersecurity and protect Federal information systems against evolving threats. As part of this effort, agencies were instructed to immediately enhance protection of Federal information and assets and improve the resilience of networks. One required action was to dramatically accelerate implementation of multifactor authentication, especially for privileged users[2]. OMB noted that requiring the use of multifactor authentication could significantly reduce the risk of adversaries compromising Federal networks and systems. As part of its effort to reinvigorate the need for PIV cards, OMB issued M-16-04, *Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government*, which required agencies to utilize PIV cards for all privileged user accounts and 85 percent of standard user accounts by September 30, 2016. While our review closely follows the recent release of new OMB requirements related to PIV card implementation, our review considered all requirements and guidance related to multifactor authentication and PIV card implementation, including guidance issued prior to the Cybersecurity Sprint.

We reviewed 18 Federal information systems, which included Federal systems operated by contractors, at 5 locations, including Department Headquarters, Y-12 National Security Complex (Y-12), Savanah River Site, Pacific Northwest National Laboratory, and the National Renewable Energy Laboratory. Although we determined that officials had implemented certain aspects of multifactor authentication at the time of our reviews, we found that none of the sites reviewed had fully implemented multifactor authentication requirements such as PIV card access or authentication risk assessments for network, local, and/or remote access according to Federal requirements for privileged and/or standard users. We also found that locations reviewed had not always considered multifactor authentication controls over applications, including those potentially containing sensitive information. Furthermore, we determined that information reported to OMB by the Department related to progress implementing the Cybersecurity Sprint was not consistent and did not portray an accurate accounting of its use of multifactor authentication.

[1] A list of related criteria is included in Appendix 2.

[2] At the time of our test work, the Office of the Chief Information Officer defined privileged users as having elevated functions, such as system, network, security, and database administrators, as well as other information technology personnel with the need to manage the security and administration of an information system. A standard user typically does not have elevated privileges above those required for the daily performance of their duties, such as a general purpose business system user in office computing environments.

Network, Local, and Remote Access

At the time of our test work, none of the five locations reviewed had fully implemented multifactor authentication for network and local access[3] in accordance with applicable Federal requirements. Contrary to OMB requirements, our review determined that none of the sites reviewed had fully implemented PIV cards for privileged and/or standard user accounts when accessing network assets. For example, at the time of our visit, privileged and standard users at Y-12 used either usernames and passwords or tokens, but not PIV cards to authenticate to network resources. In responding to our findings, management asserted that it had increased the use of PIV cards subsequent to our test work to meet Department goals. In addition, rather than using PIV cards, the Savannah River Site used RSA security tokens for the majority of privileged users to access its network at the time of our test work. Most standard users at the site authenticated using only a username and password. Office of Environmental Management officials noted that significant progress had been made subsequent to our review and that all privileged and standard users under the program’s cognizance had transitioned to PIV cards. Similarly, the National Nuclear Security Administration reported to the Office of the Chief Information Officer (OCIO) that it had recently implemented PIV cards for the majority of Savannah River Site users. Although the National Institute of Standards and Technology required multifactor authentication to be applied to certain types of local systems, such as those with elevated risk levels, our review also demonstrated that none of the five sites reviewed had addressed multifactor authentication on local systems, including systems used to manage critical site functions. During our review, the OCIO noted that the Department should extend the targeted multifactor authentication implementation strategy used for network accounts to address OMB multifactor authentication requirements for all accounts and systems. Implementation of network and local PIV card multifactor authentication could significantly reduce unauthorized access to valuable resources and help to minimize other risks such as insider threats.

In addition to the issues noted above, we determined that none of the locations had fully implemented OMB requirements to complete the e-authentication process for determining whether PIV cards should be implemented to allow remote access to Federal systems. Specifically, OMB M-04-04, *E-Authentication Guidance for Federal Agencies*, (December 2003) required agencies to identify and analyze the risks associated with each step of the authentication process, including conducting risk assessments, mapping identified risks to assurance levels, selecting and implementing remote access technologies based on the applicable assurance level, and assessing the implementation of selected technologies. The first step of the e-authentication process[4] requires agencies to conduct e-authentication risk assessments on

[3] Network access is access to an information system by a user communicating through a network such as a local area network, wide area network, or the Internet. Local access is access to an organization’s information system by a user communicating through a direct connection without the use of a network, such as a stand-alone workstation.

[4] The e-authentication process consists of the following 5 steps: (1) Conduct a risk assessment of the e-government system; (2) Map identified risks to the applicable assurance level; (3) Select technology based on e-authentication technical guidance; (4) Validate that the implemented system has achieved the required assurance level; and (5) Periodically reassess the system to determine technology refresh requirements.

electronic transactions to determine the appropriate level of access assurance. OMB established four identity authentication assurance levels:

OMB Identified Assurance Levels for Authentication

Assurance Level	Confidence Level	Multifactor-Authentication	Requirements
1	Little or no confidence in the asserted identity's validity.	No	No specific requirement to uniquely identify and track users.
2	Some confidence in the asserted identity's validity.	No	User shall identify by established criteria, such as User ID and Password.
3	High confidence in the asserted identity's validity.	Yes	Requires identity proofing and a secure multi-factor authentication token. Typically, a hardware token such as an RSA Token.
4	Very high confidence in the asserted identity's validity.	Yes	Requires stringent identity proofing and secure multi-factor authentication hardware token. PIV cards can meet this requirement.

However, none of the locations reviewed had adequately completed the five-step e-authentication process at the time of our test work. While some sites had addressed portions of the five-step process, we noted weaknesses with each approach and did not consider the assessments adequate. For example, although the Office of Environment, Health, Safety and Security effectively assigned assurance levels to the three systems we reviewed, we were unable to verify that the assurance levels had been validated and periodically reassessed for effectiveness. At NREL, we noted that assurance levels were assigned for each system, but adequate documentation to illustrate the mapping of risks to assurance levels or the validation and reassessment of the current assurance levels were not provided. Notably, National Renewable Energy Laboratory officials acknowledged that the site's e-authentication process needed to be reevaluated in the near future. In addition, OCIO officials and Y-12 and PNNL contractor officials stated that the e-authentication process was either not a high priority or believed it was not an established requirement. PNNL officials stated that OMB guidance pertaining to e-authentication requirements was not explicitly identified in contract requirements. However, we found that PNNL operated an information system which contained Official Use Only information and included several applications that provided support for business and project-funded collaborative efforts.

Application Access

Although multifactor authentication may not always be required for applications, we found that four of five locations reviewed had not considered multifactor authentication controls – such as PIV cards – over applications, including those containing sensitive information. While we did not make a determination regarding any specific application's need for additional authentication, we did note that the locations reviewed had not adequately considered applications when managing site authentication requirements. In light of past security breaches of sensitive systems at the Department and the Office of Personnel Management, we believe that consideration of enhanced authentication requirements for applications should have been afforded a higher level of attention. During our review, officials at several sites stated that the requirements included in recent Federal directives were primarily focused on network and remote access and, in light of the implementation deadline, their focus at the time of our audit was to address those concerns. In addition, although the Department's Multifactor Authentication Implementation Approach (MFAIA) did not include multifactor authentication for applications in its current short-term plans, it did note the intent to evaluate its applicability to applications in the future. However, given the significant amount of time that Federal multifactor authentication requirements had been in existence prior to establishment of the updated OMB requirements, we believe that the Department had sufficient time to review applications for any additional authentication needs, as appropriate.

The National Institute of Standards and Technology noted that in addition to enforcing authorized access at the information system level, many applications and services that support organizational missions and business operations can also benefit from increased information security. Specifically, the National Institute of Standards and Technology recommended that organizations employ risk-based identification and authentication mechanisms at the application level, when necessary, to provide increased information security. However, we found that three of the five sites reviewed had not adequately considered multifactor authentication options for applications even though they operated systems that contained sensitive information such as personally identifiable information and/or personal health information. For instance, one application at Y-12 contained both personally identifiable information and personal health information, privileged and standard users authenticated to the application using only their username and password. Y-12 contractor officials informed us that no reviews for the specific application had been conducted to ensure the current authentication level was sufficient.

It is critical that upon successful completion of the current implementation of multifactor authentication for network accounts that the Department turn its attention to the remaining OMB requirements, including multifactor authentication for applications.

Cybersecurity Sprint Initiative

In response to a cybersecurity breach at the Office of Personnel Management and a lack of progress by Federal agencies in implementing multifactor authentication, OMB established the Cybersecurity Sprint, a 30-day initiative that required agencies to accelerate the implementation of existing Federal requirements for multifactor authentication and report to OMB and the

Department of Homeland Security on progress and challenges by July 12, 2015. At the time the Cybersecurity Sprint was initiated, the Department reported that only 13 percent of privileged users and 11 percent of standard users were meeting the multifactor authentication requirements, resulting in the lowest ranking out of the 24 participating Federal agencies. As a result of the Cybersecurity Sprint, OMB directed the use of PIV cards by all privileged users and 85 percent of standard users when accessing Federal networks and systems, including those operated by contractors. In June 2016, approximately 1 year after the launch of the Cybersecurity Sprint initiative, the Department reported that the use of multifactor authentication, specifically PIV cards, had increased to 57 percent for privileged users and 21 percent for standard users.

Our review identified potential discrepancies with the information reported by the Department that illustrated inconsistencies and may have resulted in the misrepresentation of its progress. In particular, we found that some sites developed their own definitions of what constituted a standard and privileged user, which were not always consistent with the Department's definitions included in the MFAIA. For example, PNNL's definition of a standard account included in documentation provided during our review included staff who operate at elevated privileges on personal workstations or non-enterprise infrastructure systems and applications, while the OCIO had initially defined standard account users as organizational users who did not have elevated privileges. The differing interpretations of what defined a standard user could have resulted in users being excluded for one site but included in the reported data for another. In addition, we identified sites that had varying interpretations regarding whether they were required to report the number of accounts or users. This could have resulted in the misrepresentation of the Department's progress in implementing multifactor authentication. For instance, if a privileged user had 10 accounts associated to a single user name, it could potentially lead to some sites counting all 10 accounts; whereas, other sites would only count it as a single user, resulting in inconsistent reporting. Management commented that Department leadership made an explicit decision to measure progress based on accounts rather than users. However, we found that better communication of the multifactor authentication reporting requirements could have ensured a more consistent understanding by the Department.

We also determined that the Department had established four categories of exceptions to OMB requirements, which resulted in a significant number of exceptions to multifactor authentication requirements. In particular, as of April 2017, the Department had approved over 65,000 user account exceptions to multifactor authentication requirements based on both OMB exemptions and the newly-created Department exception categories, which officials noted accounted for about 30 percent of all network accounts. Specifically, the Department's MFAIA plan included an exception for standard user account access to moderate risk mission support systems in academic-like environments, which could have potentially excluded a large portion of national laboratory standard users given their strong focus on academic research and development. For example, at the time of our visit, NREL had received a site-wide exception from the site office and authorizing official for all standard users that provided an exception for approximately 2,200 user accounts from the OMB requirements. In addition, although Oak Ridge National Laboratory officials reported that they had completed standard user account multifactor authentication implementation, we noted that an exception for 9,211 user accounts (96 percent) existed. Although Department officials told us that the current exception process was approved by OMB, they were unable to provide documentation to support their assertion.

Implementation, Prioritization, and Communication

The weaknesses identified occurred, in part, because officials had not fully planned for implementation of multifactor authentication on its information systems. In addition, the Department had not established, or had not made clear and consistent, guidance and requirements related to the implementation of multifactor authentication technologies. Furthermore, we identified a number of communication issues that contributed to the weaknesses noted during our review.

Planning and Guidance

The Department had not adequately planned for the effective implementation of multifactor authentication on its information systems. In response to OMB direction, the Department issued Order 206.2, *Identity, Credential, and Access Management (ICAM)*, in February 2013 to support ICAM as its enterprise access and authentication management service for the verification of individuals requiring access to Department facilities and information systems. However, at the time of our test work, we noted limited progress related to the planning and implementation of ICAM and found that the limited progress directly impacted the sites' ability to plan and implement PIV card authentication. Notably, Department officials indicated that ICAM began providing authentication and access services to a limited number of program elements in April 2016. In response to our findings, management indicated that the ICAM program furthered its implementation, providing the foundation to extend multifactor authentication access to applications across the enterprise.

In addition, the Department had not yet approved its MFAIA in response to the Cybersecurity Sprint. Such a plan could have helped programs and sites prepare to meet Federal requirements by providing a detailed strategy and direction needed to finalize planning and begin implementing PIV card authentication controls. For example, Y-12 contractor officials informed us that their implementation efforts were on hold due to a lack of detailed planning and technical guidance from the Department. According to the OCIO, each program office was required to provide guidance to their sites that aligned with the Department's distributed risk management framework. Although Y-12 had initiated development of a multifactor authentication capability, it lacked the technical specifics related to the Department's ICAM initiative and other Department requirements. Y-12 contractor personnel noted that they could complete development of a multifactor authentication capability without Department guidance, but believed that doing so increased the risk that it would not be compatible with future Department provided enterprise services or would not meet specific Department requirements. Y-12 contractors also stated that the site's multifactor authentication capability could have been modified to meet PIV card requirements and the September 30, 2016 deadline as long as Department guidance had been provided in a timely manner. In response to our findings, National Nuclear Security Administration management indicated that additional Department direction is needed in regard to expectations for circumstances in which visitors or subcontractors do not have PIV credentials.

We also identified concerns related to whether adequate funding existed to support the effective implementation of multifactor authentication. Officials at each of the sites reviewed expressed concern over the lack of additional funding for multifactor authentication and stated that funding constraints had negatively impacted current and previous implementation attempts. However, none of the sites could provide supporting documentation pertaining to requests for funding the initiative. Furthermore, several sites indicated that they would be required to reprioritize cybersecurity projects and initiatives that they believed to be of potentially higher risk and priority than multifactor authentication. Interestingly, as noted in our prior report on *The Department of Energy's Implementation of Homeland Security Presidential Directive 12* (DOE/IG-0860, February 2012), OMB had previously directed that beginning in fiscal year 2012, development and technology refresh funding would be limited to HSPD-12 implementation activities until the PIV card was completely implemented. However, based on our reviews of several system development efforts in recent years, we concluded that the Department continued to develop information systems without implementing the OMB directive.

In addition, OCIO officials informed us that the Department had requested additional funding from OMB for the implementation of multifactor authentication in October 2015 but the additional funding was not made available. One OCIO official stated, but could not provide documentation to support, that OMB informed the Department that funding for the initiative had been included in budget allocations over the course of the past 10 years. OCIO officials added that they believed there was sufficient funding to support multifactor implementation efforts and as a result, the Deputy Secretary directed program offices to implement multifactor authentication by reprioritizing and reallocating existing funding, as necessary. We found that although Federal and contractor officials provided varying opinions on funding for multifactor authentication efforts, it became apparent that improved financial planning could have helped the Department meet authentication requirements.

The weaknesses identified during our review existed even though Federal requirements for multifactor authentication had been established more than 10 years prior to our audit. For example, in 2004 and 2011, OMB issued requirements pertaining to the implementation of HSPD-12, including the use of PIV cards for Federal and contractor employees. In addition, OMB[5] required that each agency develop and issue a PIV card implementation policy by March 31, 2011, through which the agency would require the use of PIV cards as the common means of authentication for access to facilities, networks, and information systems. However, as noted in our report, while many locations used tokens to access information systems, they had not fully implemented PIV card multifactor authentication.

[5] OMB M-11-11, Continued Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors

The Department reported in its June 2016 MFAIA update that it had increased its multifactor authentication implementation goal for standard users from 85 to 100 percent. However, we also noted that the Department had increased the number of exceptions to Federal multifactor authentication requirements in the MFAIA, adding four additional exception categories to established OMB requirements. Although unable to provide support, OCIO officials stated that the MFAIA, including the exception process, had been presented to and approved by OMB and Department management. While the Department faces significant challenges with the implementation of multifactor authentication, we believe the current MFAIA, notably the exception process, and Department Order 206.2 are both in conflict with OMB requirements pertaining to PIV card implementation.

Communication

We identified a number of communication weaknesses that contributed to the Department's limited progress regarding multifactor authentication implementation. For example, communication issues existed between Department and contractor officials regarding the requirements for multifactor authentication. Officials at several sites stated that Federal requirements for multifactor authentication were not included in their contracts and/or they were not officially notified by Federal officials to implement multifactor authentication. However, as directed in HSPD-12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, and Federal Information Processing Standard 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, contractors generally have been required to implement and follow multifactor authentication requirements since 2004.

Although the OCIO indicated that various mechanisms were established to enable communication, officials we spoke with noted a lack of effective communication related to various issues identified in our report. For example, contractor officials at several sites stated that, in some instances, they were unsure of whom to contact if they had questions or concerns regarding multifactor authentication. Several Federal Site Offices expressed similar concerns, indicating that while contractors would communicate certain issues to them, they were also uncertain of whom they should contact to help address issues. In addition, officials at some Federal Site Offices noted instances in which they would elevate concerns to Headquarters and the responses they received would be sporadic or would not receive a response. As a result, we concluded that enhanced communication could have addressed issues for several sites across the Department and led to a more efficient implementation of multifactor authentication.

Similarly, we determined that a lack of well-defined reporting criteria hindered the reporting of Cybersecurity Sprint information. We found that there was significant confusion when the initiative was established regarding whether sites were to report the number of users or accounts that were or should be utilizing multifactor authentication. In addition, there was confusion regarding the definition of what was considered a privileged user and what was considered a standard user. Site officials commented that these concerns were brought up to the OCIO and some were eventually addressed over the course of the initiative. However, we observed that there was still confusion regarding the reporting of accounts and users, as well as what was considered a privileged and standard user.

Impact and Path Forward

Until the Department adequately implements, prioritizes, and communicates Federal requirements, it will continue to put its information systems and related data at a higher-than-necessary risk of compromise. In addition, without improved communication and consideration of key multifactor authentication budget priorities, such as communicating funding options, defining key processes, and implementing enterprise provided services, the Department will continue to struggle with its multifactor authentication implementation. Furthermore, until data call reporting criteria is better defined and communicated, the Department will continue to report inconsistent data to the relevant authorities, not only for the Cybersecurity Sprint, but also for future data calls and initiatives.

RECOMMENDATIONS

To help improve the Department's implementation of multifactor authentication, we recommend that the Administrator for the National Nuclear Security Administration, Acting Under Secretary for Science and Energy, and Acting Under Secretary for Management and Performance, in coordination with the Department of Energy and National Nuclear Security Administration Chief Information Officers, as appropriate:

1. Ensure that multifactor authentication and future implementation plans are fully developed, approved, and fully documented in a timely manner and communicated to all programs, sites, and contractors, as appropriate;

2. Ensure that implementation of multifactor authentication and future projects are adequately considered as part of the development of budget priorities;

3. Ensure that information related to the implementation of the Department's multifactor authentication and future efforts are effectively communicated to all relevant stakeholders by resolving existing communication weaknesses between Headquarters and site locations, including contractors;

4. Ensure all applicable contractual requirements are accurate, clearly communicated, and understood by all stakeholders and enforced enterprise-wide; and

5. Ensure the Multifactor Authentication Implementation Approach and Department policies and guidance related to PIV card implementation are implemented in accordance with established Federal requirements and directives.

MANAGEMENT RESPONSE

Management concurred with each of the report's recommendations and indicated that corrective actions had been initiated or were planned to address the issues identified in the report. Management also emphasized that the Department has used various forms of multifactor authentication over the years and noted that PIV credentials are only one form of multifactor authentication. In response to our recommendations, management indicated that it is developing a targeted plan of action to specifically address the outstanding user accounts not currently using Level of Assurance 4 credentials. Furthermore, management indicated that, as Federal requirements change, the Department plans to respond by updating policies to reflect the latest guidance and ensuring that requirements are appropriately communicated to all stakeholders and actions are taken to make the necessary contract modifications. Management commented that it is also developing a detailed plan of action and milestones outlining specific plans to reach Department goals related to multifactor authentication.

AUDITOR COMMENTS

Management's comments and planned corrective actions were responsive to our recommendations. Management's comments are included in Appendix 4.

OBJECTIVE, SCOPE, AND METHODOLOGY

Objective

To determine whether the Department of Energy effectively implemented multifactor authentication when securing its information systems.

Scope

The scope was limited to evaluating the Department's implementation of multifactor authentication and applicable requirements. The audit was performed between October 2015 and September 2017 at five locations, including Department Headquarters in Germantown, Maryland and Washington, DC; Y-12 National Security Complex in Oak Ridge, Tennessee; Savanah River Site in Aiken, South Carolina; Pacific Northwest National Laboratory in Hanford, Washington; and the National Renewable Energy Laboratory in Golden, Colorado. We reviewed a total of 18 different information systems at the 5 locations. The audit was conducted under Office of Inspector General project number A16TG003.

Methodology

To accomplish our objective, we:

- Reviewed applicable Federal and Department standards and guidance, including National Institute of Standards and Technology and Office of Management and Budget requirements;

- Reviewed prior reports issued by the Office of Inspector General and Government Accountability Office and determined the status of prior recommendations;

- Held discussions with Department and contractor personnel at each of the locations reviewed regarding the implementation of multifactor authentication and objectives of our audit;

- Requested and reviewed Department and site specific documentation pertaining to the implementation of multifactor authentication; and

- Reviewed the application of multifactor authentication for information systems at each of the sites reviewed, including the application of cybersecurity controls pertaining to multifactor authentication.

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 objective. We believe the evidence obtained provides a reasonable basis for our findings and conclusion based on our objective. Accordingly, we assessed significant internal controls and compliance with laws and regulations to the extent necessary to satisfy the audit objective. In particular, we assessed the Department's implementation of the *GPRA Modernization Act of 2010* and determined that it had established performance measures and/or goals related to multifactor authentication. Because our review was limited, it would not have necessarily disclosed all internal control deficiencies that may have existed at the time of our audit. We did not rely on computer-processed data to satisfy our objective.

An exit conference was held with management on September 13, 2017.

RELATED CRITERIA

Related HSPD-12/PIV Card Criteria	Issuance Date
Clause 48 CFR 970.5204-2 Laws, Regulations, and Department of Energy Directives	December 2000
Clause 48 CFR 52.204-9 Personal Identity Verification of Contractor Personnel	November 2006
Office of Management and Budget (OMB) M-04-04, E-Authentication Guidance for Federal Agencies	December 16, 2003
Homeland Security Presidential Directive 12 (HSPD-12): *Policy for a Common Identification Standard for Federal Employees and Contractors*	August 27, 2004
OMB M-05-24, *Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors*	August 5, 2005
OMB M-07-06, *Validating and Monitoring Agency Issuance of Personal Identity Verification Credentials*	January 11, 2007
OMB M-08-01, *HSPD-12 Implementation Status*	October 23, 2007
OMB M-11-11, *Continued Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors*	February 3, 2011
Department Order 206.2, *Identity, Credential, Access Management (ICAM)*	February 19, 2013
Public Law 113-283: *Federal Information Security Modernization Act of 2014*	December 18, 2014
Department of Energy Order 205.1B Chg. 3: *Department of Energy Cyber Security Program*	April 29, 2014
OMB M-16-04, *Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government*	October 30, 2015

PRIOR REPORTS

- Evaluation Report on *The Department of Energy's Unclassified Cybersecurity Program – 2015* (DOE-OIG-16-01, November 2015). The report noted that the Department of Energy made significant progress in remediating weaknesses identified in our fiscal year 2014 evaluation, which resulted in the closure of 22 of 26 reported deficiencies. While these actions were positive, our current evaluation found that the types of deficiencies identified in prior years, such as issues related to security reporting, vulnerability management, system integrity of Web applications, and account management continued to persist. Specifically, contrary to management's response to our prior year's evaluation, the Department did not report the status of its entire cybersecurity program to the Department of Homeland Security, officials continued to excluded contractor systems in their reporting. Weaknesses existed related to system integrity of Web applications, including human resources, financial, and business applications. We found that applications accepted malicious input data that could have been used to launch attacks against application users. In addition, applications at a number of locations stored user authentication information in an unsecure manner. Additionally, access control and segregation of duties weaknesses and opportunities for improvement were identified at five locations and weaknesses continued to exist related to vulnerability management. The weaknesses identified occurred, in part, because the Department had not ensured that policies and procedures were fully developed and/or implemented to meet all necessary cybersecurity requirements. In addition, the Department had not always implemented an effective performance monitoring and risk management program.

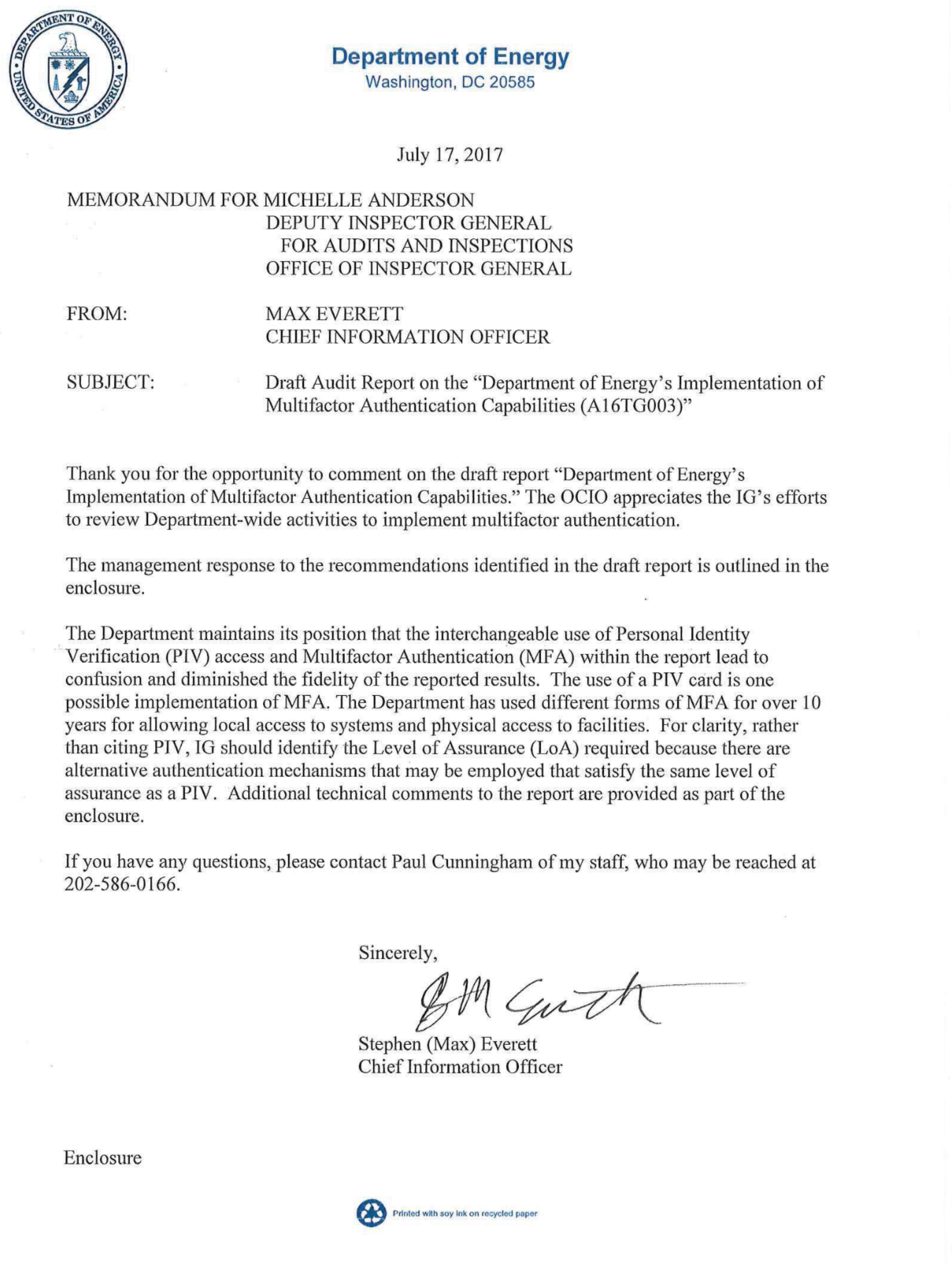
- Special Report on *The Department of Energy's July 2013 Cyber Security Breach* (DOE/IG-0900, December 2013). The review identified a number of technical and management issues that contributed to an environment in which the breach was possible. For example, contrary to Federal guidance, social security numbers were frequently used as identifiers, and security planning and testing activities were not conducted as required. In addition, systems were permitted to operate even though they were known to have security vulnerabilities and less than adequate security controls. Furthermore, there was a failure to assign the appropriate level of urgency to replacing end-of-life systems, leaving one system in operation 8 months after support for the system had ended. While a single point of failure for the breach was not identified, the combination of the technical and managerial problems observed contributed to the incident occurring. Numerous contributing factors related to inadequate management processes were identified. These included competing priorities between mission-related work and cybersecurity, unclear lines of responsibility, lack of awareness by responsible officials of the operating environment, and ineffective coordination and communications. The report noted that the Department needed to revamp its Headquarters' cybersecurity program and control environment, as well as enhance communications and coordination. To help address these issues, a number of recommendations were made designed to improve security for Department information.

- Audit Report on *The Department of Energy's Implementation of Homeland Security Presidential Directive 12* (DOE/IG-0860, February 2012). The audit found that the Department, despite years of effort and expenditures of more than $15 million, had not met all Homeland Security Presidential Directive (HSPD) 12 requirements. In particular, the Department had not fully implemented physical and logical access controls in accordance with HSPD-12. Furthermore, the Department had not issued HSPD-12 credentials to many uncleared contractor personnel at its field sites. These issues occurred, at least in part, because there was a lack of a coordinated approach among programs and sites related to implementation of the HSPD-12 requirements. In particular, guidance provided by management was fragmented and often inadequate to meet the goals of the initiative. In addition, ongoing efforts suffered from a lack of coordination among programs and sites to determine the cost, scope, and schedule of work required to implement HSPD-12 requirements. Further, several programs and sites visited had not established budgets in an attempt to obtain funding to support HSPD-12 activities. There were a number of recommendations made to improve the Department's ability to effectively implement physical and logical access controls in accordance with HSPD-12.

- Audit Report on the *Security Over Personally Identifiable Information* (DOE/IG-0771, July 2007). The audit report noted that the Department maintained numerous information systems that contained personally identifiable information and found that required Federal protective measures had not been fully implemented. Specifically, not all Office of Management and Budget and National Institute of Standards and Technology requirements had been incorporated into relevant documents. In addition, when policies were clear, programs and sites did not always enforce the requirements to ensure that necessary controls were in place for protecting Personally Identifiable Information. We noted that without improvements in policy development and implementation, the Department would have difficult time securing personal information. In addition, there was a less-than-acceptable risk that affected individuals would not be notified if their personal information was exposed. The report noted that these issues occurred due to ineffective and unenforced policies, and until protective measures were fully implemented, the Department could have difficulty protecting personal information. To address the identified issues, several recommendations were made intended to help secure Personally Identifiable Information.

APPENDIX 4

MANAGEMENT COMMENTS



Department of Energy
Washington, DC 20585

July 17, 2017

MEMORANDUM FOR MICHELLE ANDERSON
DEPUTY INSPECTOR GENERAL
FOR AUDITS AND INSPECTIONS
OFFICE OF INSPECTOR GENERAL

FROM: MAX EVERETT
CHIEF INFORMATION OFFICER

SUBJECT: Draft Audit Report on the "Department of Energy's Implementation of Multifactor Authentication Capabilities (A16TG003)"

Thank you for the opportunity to comment on the draft report "Department of Energy's Implementation of Multifactor Authentication Capabilities." The OCIO appreciates the IG's efforts to review Department-wide activities to implement multifactor authentication.

The management response to the recommendations identified in the draft report is outlined in the enclosure.

The Department maintains its position that the interchangeable use of Personal Identity Verification (PIV) access and Multifactor Authentication (MFA) within the report lead to confusion and diminished the fidelity of the reported results. The use of a PIV card is one possible implementation of MFA. The Department has used different forms of MFA for over 10 years for allowing local access to systems and physical access to facilities. For clarity, rather than citing PIV, IG should identify the Level of Assurance (LoA) required because there are alternative authentication mechanisms that may be employed that satisfy the same level of assurance as a PIV. Additional technical comments to the report are provided as part of the enclosure.

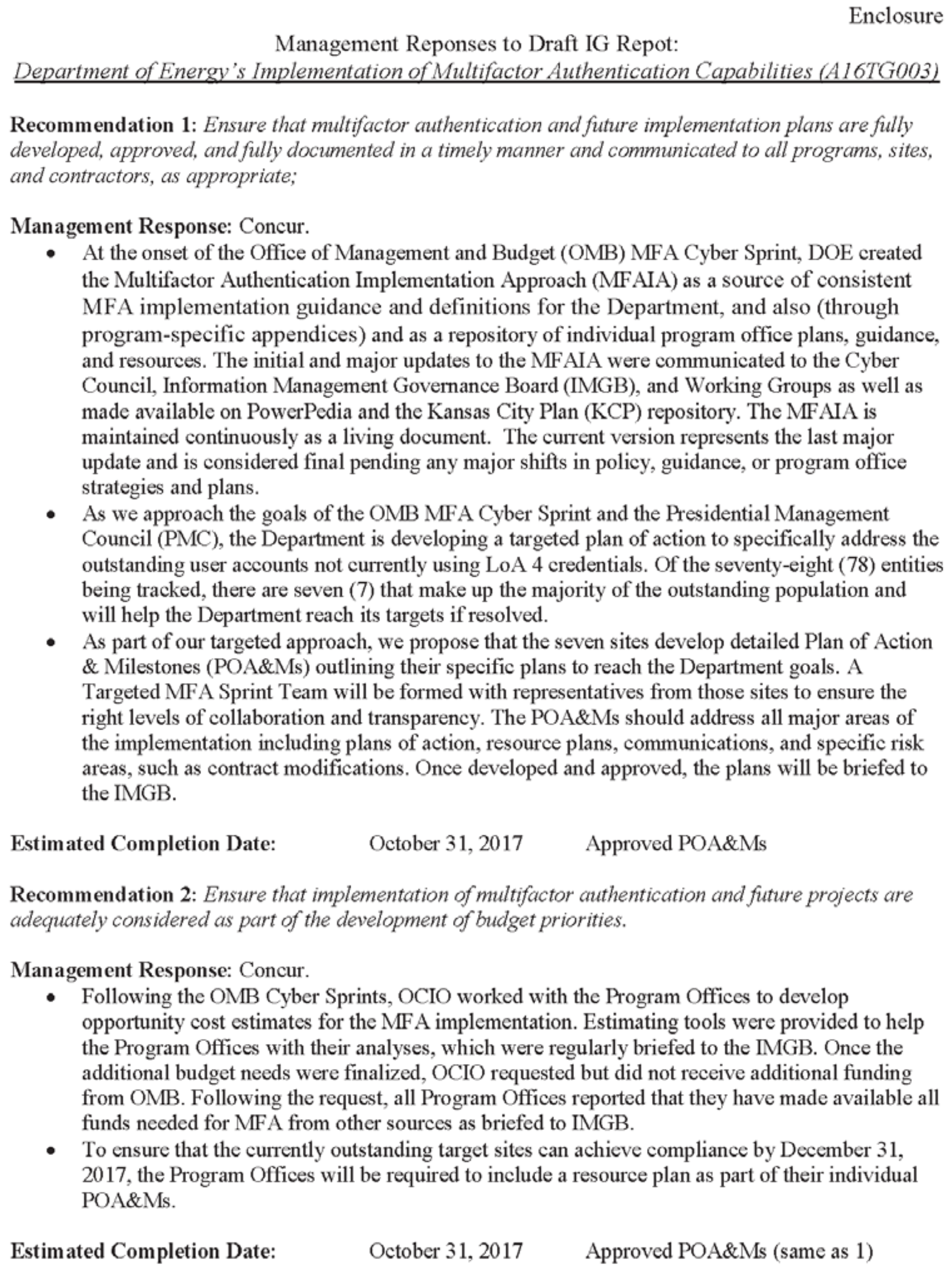
If you have any questions, please contact Paul Cunningham of my staff, who may be reached at 202-586-0166.

Sincerely,

Stephen (Max) Everett
Chief Information Officer

Enclosure

Printed with soy ink on recycled paper



Enclosure

Management Reponses to Draft IG Repot:

Department of Energy's Implementation of Multifactor Authentication Capabilities (A16TG003)

Recommendation 1: *Ensure that multifactor authentication and future implementation plans are fully developed, approved, and fully documented in a timely manner and communicated to all programs, sites, and contractors, as appropriate;*

Management Response: Concur.

- At the onset of the Office of Management and Budget (OMB) MFA Cyber Sprint, DOE created the Multifactor Authentication Implementation Approach (MFAIA) as a source of consistent MFA implementation guidance and definitions for the Department, and also (through program-specific appendices) and as a repository of individual program office plans, guidance, and resources. The initial and major updates to the MFAIA were communicated to the Cyber Council, Information Management Governance Board (IMGB), and Working Groups as well as made available on PowerPedia and the Kansas City Plan (KCP) repository. The MFAIA is maintained continuously as a living document. The current version represents the last major update and is considered final pending any major shifts in policy, guidance, or program office strategies and plans.
- As we approach the goals of the OMB MFA Cyber Sprint and the Presidential Management Council (PMC), the Department is developing a targeted plan of action to specifically address the outstanding user accounts not currently using LoA 4 credentials. Of the seventy-eight (78) entities being tracked, there are seven (7) that make up the majority of the outstanding population and will help the Department reach its targets if resolved.
- As part of our targeted approach, we propose that the seven sites develop detailed Plan of Action & Milestones (POA&Ms) outlining their specific plans to reach the Department goals. A Targeted MFA Sprint Team will be formed with representatives from those sites to ensure the right levels of collaboration and transparency. The POA&Ms should address all major areas of the implementation including plans of action, resource plans, communications, and specific risk areas, such as contract modifications. Once developed and approved, the plans will be briefed to the IMGB.

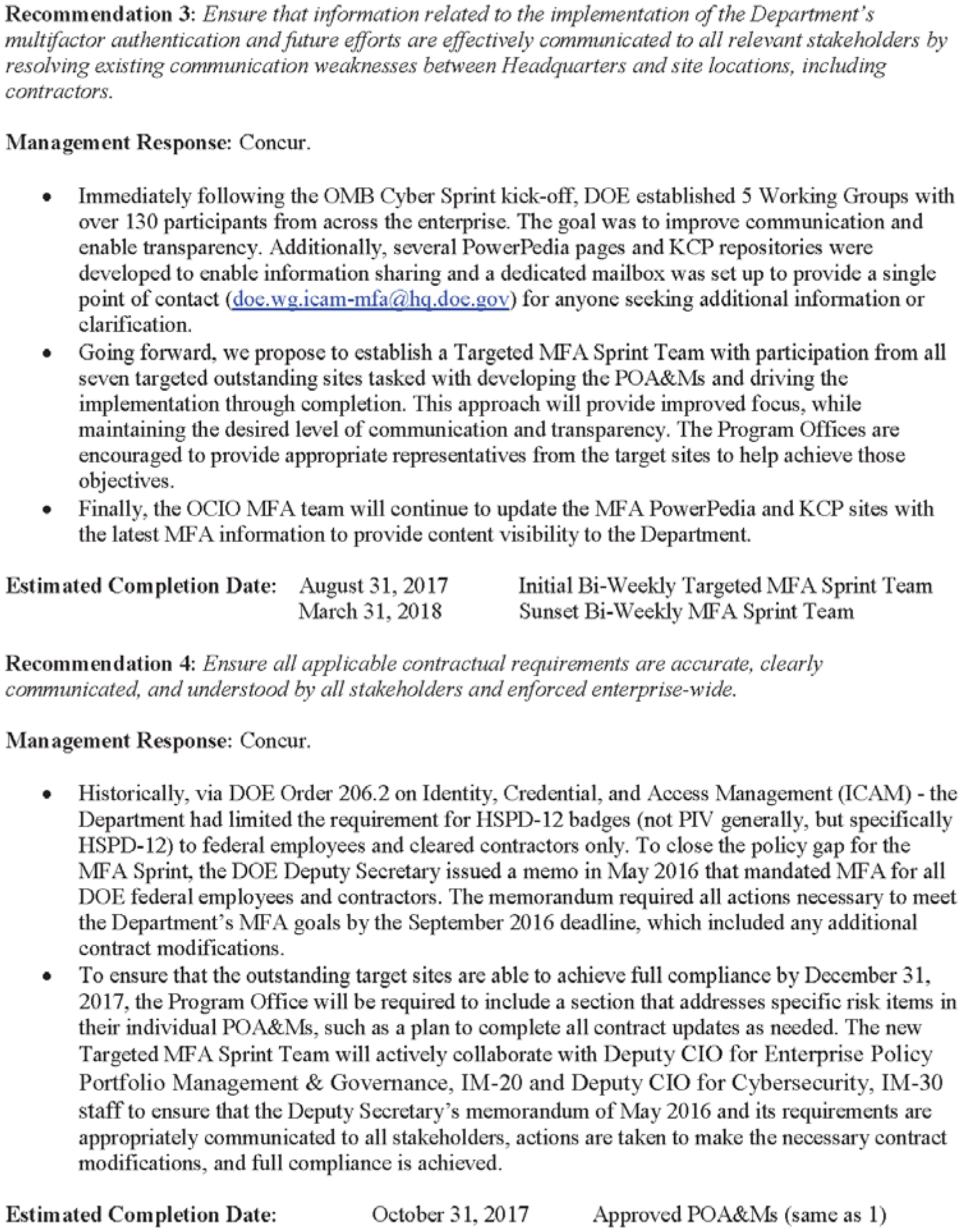
Estimated Completion Date: October 31, 2017 Approved POA&Ms

Recommendation 2: *Ensure that implementation of multifactor authentication and future projects are adequately considered as part of the development of budget priorities.*

Management Response: Concur.

- Following the OMB Cyber Sprints, OCIO worked with the Program Offices to develop opportunity cost estimates for the MFA implementation. Estimating tools were provided to help the Program Offices with their analyses, which were regularly briefed to the IMGB. Once the additional budget needs were finalized, OCIO requested but did not receive additional funding from OMB. Following the request, all Program Offices reported that they have made available all funds needed for MFA from other sources as briefed to IMGB.
- To ensure that the currently outstanding target sites can achieve compliance by December 31, 2017, the Program Offices will be required to include a resource plan as part of their individual POA&Ms.

Estimated Completion Date: October 31, 2017 Approved POA&Ms (same as 1)



Recommendation 3: *Ensure that information related to the implementation of the Department's multifactor authentication and future efforts are effectively communicated to all relevant stakeholders by resolving existing communication weaknesses between Headquarters and site locations, including contractors.*

Management Response: Concur.

- Immediately following the OMB Cyber Sprint kick-off, DOE established 5 Working Groups with over 130 participants from across the enterprise. The goal was to improve communication and enable transparency. Additionally, several PowerPedia pages and KCP repositories were developed to enable information sharing and a dedicated mailbox was set up to provide a single point of contact (doe.wg.icam-mfa@hq.doe.gov) for anyone seeking additional information or clarification.
- Going forward, we propose to establish a Targeted MFA Sprint Team with participation from all seven targeted outstanding sites tasked with developing the POA&Ms and driving the implementation through completion. This approach will provide improved focus, while maintaining the desired level of communication and transparency. The Program Offices are encouraged to provide appropriate representatives from the target sites to help achieve those objectives.
- Finally, the OCIO MFA team will continue to update the MFA PowerPedia and KCP sites with the latest MFA information to provide content visibility to the Department.

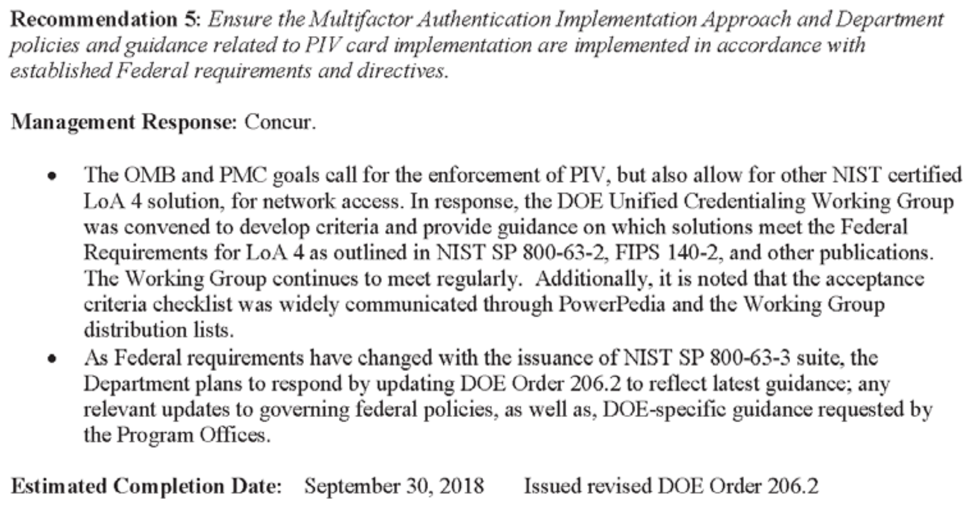
Estimated Completion Date:	August 31, 2017	Initial Bi-Weekly Targeted MFA Sprint Team
	March 31, 2018	Sunset Bi-Weekly MFA Sprint Team

Recommendation 4: *Ensure all applicable contractual requirements are accurate, clearly communicated, and understood by all stakeholders and enforced enterprise-wide.*

Management Response: Concur.

- Historically, via DOE Order 206.2 on Identity, Credential, and Access Management (ICAM) - the Department had limited the requirement for HSPD-12 badges (not PIV generally, but specifically HSPD-12) to federal employees and cleared contractors only. To close the policy gap for the MFA Sprint, the DOE Deputy Secretary issued a memo in May 2016 that mandated MFA for all DOE federal employees and contractors. The memorandum required all actions necessary to meet the Department's MFA goals by the September 2016 deadline, which included any additional contract modifications.
- To ensure that the outstanding target sites are able to achieve full compliance by December 31, 2017, the Program Office will be required to include a section that addresses specific risk items in their individual POA&Ms, such as a plan to complete all contract updates as needed. The new Targeted MFA Sprint Team will actively collaborate with Deputy CIO for Enterprise Policy Portfolio Management & Governance, IM-20 and Deputy CIO for Cybersecurity, IM-30 staff to ensure that the Deputy Secretary's memorandum of May 2016 and its requirements are appropriately communicated to all stakeholders, actions are taken to make the necessary contract modifications, and full compliance is achieved.

Estimated Completion Date:	October 31, 2017	Approved POA&Ms (same as 1)



Recommendation 5: *Ensure the Multifactor Authentication Implementation Approach and Department policies and guidance related to PIV card implementation are implemented in accordance with established Federal requirements and directives.*

Management Response: Concur.

- The OMB and PMC goals call for the enforcement of PIV, but also allow for other NIST certified LoA 4 solution, for network access. In response, the DOE Unified Credentialing Working Group was convened to develop criteria and provide guidance on which solutions meet the Federal Requirements for LoA 4 as outlined in NIST SP 800-63-2, FIPS 140-2, and other publications. The Working Group continues to meet regularly. Additionally, it is noted that the acceptance criteria checklist was widely communicated through PowerPedia and the Working Group distribution lists.
- As Federal requirements have changed with the issuance of NIST SP 800-63-3 suite, the Department plans to respond by updating DOE Order 206.2 to reflect latest guidance; any relevant updates to governing federal policies, as well as, DOE-specific guidance requested by the Program Offices.

Estimated Completion Date: September 30, 2018 Issued revised DOE Order 206.2

FEEDBACK

The Office of Inspector General has a continuing interest in improving the usefulness of its products. We aim to make our reports as responsive as possible and ask you to consider sharing your thoughts with us.

Please send your comments, suggestions, and feedback to OIG.Reports@hq.doe.gov and include your name, contact information, and the report number. You may also mail comments to us:

Office of Inspector General (IG-12)
Department of Energy
Washington, DC 20585

If you want to discuss this report or your comments with a member of the Office of Inspector General staff, please contact our office at (202) 253-2162.