INSPECTION

OFFICE OF
INSPECTOR GENERAL
U.S. DEPARTMENT OF THE INTERIOR

P@s$w0rds at the U.S. Department of the Interior: Easily Cracked Passwords, Lack of Multifactor Authentication, and Other Failures Put Critical DOI Systems at Risk

This is a revised version of the report prepared for public release.

Report No.: 2021–ITA–005

January 2023

OFFICE OF
INSPECTOR GENERAL
U.S. DEPARTMENT OF THE INTERIOR

JAN 03 2023

Memorandum

To: Darren Ash
Chief Information Officer

From: Kathleen Sedney Kathleen Sedney
Assistant Inspector General for Audits, Inspections, and Evaluations

Subject: Final Inspection Report – *P@s$w0rds at the U.S. Department of the Interior: Easily Cracked Passwords, Lack of Multifactor Authentication, and Other Failures Put Critical DOI Systems at Risk*
Report No. 2021–ITA–005

This memorandum transmits our inspection report on U.S. Department of the Interior's password complexity requirements. Our objective was to determine whether the Department's password management and enforcement controls were effective enough to prevent a malicious actor from gaining unauthorized access to Department computer systems by capturing and "cracking" user passwords.

We will refer Recommendations 1 through 8 to the Office of Policy, Management and Budget for resolution and implementation tracking and to report to us on their status. In addition, we will notify Congress about our findings, and we will report semiannually, as required by law, on actions you have taken to implement the recommendations and on recommendations that have not been implemented. We will also post a public version of this report on our website.

If you have any questions about this report, please call me at 202–208–5745.

cc: John Clink, Acting Chief Information Security Officer

Contents

Results in Brief

What We Inspected

We performed an inspection of the U.S. Department of the Interior's password complexity requirements. Our objective was to determine whether the Department's password management and enforcement controls were effective enough to prevent a malicious actor from gaining unauthorized access to Department computer systems by capturing and "cracking" user passwords. We initiated this inspection because we were able to crack between 20 and 40 percent of the passwords we captured during past projects. For this project, we decided to perform a formal test of passwords throughout the Department. We did so after defining "rules of engagement" with the Department to ensure that it was able to protect its IT systems and that any vulnerabilities could be addressed promptly.

Password-based authentication security concerns have been widely reported in both the public and private sectors. We note as one example, a 2021 article "One Stolen Password Took Down The Colonial Pipeline—Is Your Business Next?" in which *Forbes* reported that cybercriminals launched a ransomware attack on the Colonial Pipeline—"effectively shutting down half of the country's fuel supply chain—by stealing one password."[1] Specifically, the article explained the password used in the attack was found inside a batch of leaked passwords published online. According to the article, the attackers then exploited additional account management weaknesses (e.g., single-factor authentication and inactive accounts that had not been disabled) to gain unauthorized access to the company's network.

As discussed below, we found that the Department's computer system authentication mechanisms and account management practices exhibited weaknesses similar to those that were reportedly exploited in the Colonial Pipeline attack. Specifically, Department employees used passwords found on breached password lists available on the internet, the Department used single-factor authentication, and inactive accounts were not disabled. We do not assert that the Department faces the same types of risks as did Colonial Pipeline—aside from other considerations, although a breach to the Department's computer network could have a significant adverse effect on its operations, such a breach would not necessarily produce the same widespread disruption to businesses and consumers that resulted from the Colonial Pipeline IT security incident. Should the Department experience a similar attack, there is a high probability that bureau mission operations could be significantly affected. However, we did not attempt to compromise the Department's network by exploiting the vulnerabilities we found because such testing was out of scope.

[1] Endler, David. "One Stolen Password Took Down The Colonial Pipeline—Is Your Business Next?" *Forbes*, September 14, 2021. https://www.forbes.com/sites/forbestechcouncil/2021/09/14/one-stolen-password-took-down-the-colonial-pipeline---is-your-business-next/?sh=ca4b4af5f56d.

What We Found

We found that the Department's management practices and password complexity requirements were not sufficient to prevent potential unauthorized access to its systems and data. Over the course of our inspection, we cracked 18,174 of 85,944—or 21 percent of active user passwords, including 288 accounts with elevated privileges and 362 accounts of senior U.S. Government employees.

In the course of our work, we found that:

- The Department did not consistently implement multifactor authentication, including for 89 percent of its High Value Assets (assets that could have serious impacts to the Department's ability to conduct business if compromised), which left these systems vulnerable to password compromising attacks.

- The Department's password complexity requirements were outdated and ineffective, allowing users to select easy-to-crack passwords (e.g., `Changeme$12345`, `Polar_bear65`, `Nationalparks2014!`). We found, for example, that 4.75 percent of all active user account passwords were based on the word "password." In the first 90 minutes of testing, we cracked the passwords for 16 percent of the Department's user accounts.

- The Department's password complexity requirements implicitly allowed unrelated staff to use the same inherently weak passwords—meaning there was not a rule in place to prevent this practice. For example, the most commonly reused password (`Password-1234`) was used on 478 unique active accounts. In fact, 5 of the 10 most reused passwords at the Department included a variation of "password" combined with "1234"; this combination currently meets the Department's requirements even though it is not difficult to crack.

- The Department did not timely disable inactive (unused) accounts or enforce password age limits, which left more than 6,000 additional active accounts vulnerable to attack.

Why This Matters

Identifying and authenticating users is a fundamental security control for granting access to computer systems and information resources. As such, authentication methods—such as passwords—are a prime target of attack for malicious actors attempting to gain unauthorized access to sensitive data. If a malicious actor compromises an account with elevated privileges, such as the account of a system administrator, the magnitude of harm increases as the attacker can upload malware, steal sensitive data, add or delete users, change system configurations, and alter logs to conceal his or her actions.

What We Recommend

We make eight recommendations to help the Department strengthen its IT security by improving user account management practices.

Introduction

Objective

The objective of our inspection was to determine whether the U.S. Department of the Interior's password management and enforcement controls were effective enough to prevent a malicious actor from gaining unauthorized access to Department computer systems by capturing and "cracking" user passwords.

See Appendix 1 for our inspection scope and methodology.

Background

The Department's Information Security Governance Model

The Department's Chief Information Officer (CIO) is responsible for establishing Departmentwide IT security policy and overseeing implementation to ensure compliance for all information systems. The Department's Chief Information Security Officer is responsible for developing and maintaining a Departmentwide information security program as well as for carrying out the CIO's information security responsibilities. The heads of bureaus and offices are responsible for ensuring compliance with these departmental policies and procedures, as well as any applicable Federal laws, rules, regulations, policies, standards, and procedures.[2]

Department Computer System Authentication Mechanisms

The Department uses two types of authentication to grant access to computer systems: single-factor authentication and multifactor authentication (MFA).[3] MFA refers to the requirement to use at least two factors to access computer systems; as discussed in more detail below, MFA has been required on Federal information systems for nearly two decades.

MFA May Include:

Something the user *knows*	=	passwords or personal identification numbers (**PINs**)
Something the user *has*	=	cryptographic identification devises such as personal identity verification (**PIV**) cards or tokens
Something the user *is*	=	unique biometric characteristics such as fingerprints or retinal patterns

[2] See 375 *DM* 19, "Information Security Program," issued March 21, 2012, available at https://www.doi.gov/sites/doi.gov/files/elips/documents/375-dm-19_0.pdf.

[3] See the National Institute of Standards and Technology's MFA definitions at https://csrc.nist.gov/glossary/term/Multi_Factor_Authentication.

Most recently, Executive Order No. 14028, *Improving the Nation's Cybersecurity*, issued on May 12, 2021, mandated the widespread implementation of MFA by November 8, 2021.[4] Pursuant to this order, MFA is required on all Federal information systems, wherever possible, and exceptions must be documented and sent to Cybersecurity and Infrastructure Security Agency.

The Department primarily uses a Microsoft Active Directory (AD) infrastructure to identify and authenticate users and approve access to digital resources, such as bureau computer systems and data.[5] Microsoft AD is a Windows domain service that combines authentication, authorization, and directory technologies to centralize system administration and secure computer systems.

The most common MFA method the Department has implemented within the AD is a PIV card issued to all employees, which combines a digital certificate contained on the card and a PIN set by each employee. When this MFA method is properly implemented, employees do not need to use their AD password.

The Office of the Chief Information Officer (OCIO) documents its minimum control requirements in internally published documents it calls Security Control Standards. Departmentwide password complexity requirements are defined in the *Security Control Standard: Identification and Authentication* (Version 4.1, dated September 2016). The standard states that passwords used for single-factor authentication must have a minimum length of 12 characters and contain at least 3 of 4 character types consisting of uppercase, lowercase, digits, and special characters. The Department also requires users to change their passwords every 60 days.

According to the National Institute of Standards and Technology (NIST) Special Publication 800–63, *Digital Identity Guidelines* (SP 800–63) document suite,[6] relying on usernames and passwords alone (i.e., single-factor authentication) greatly increases the risk to computer systems because it is much easier for an attacker to obtain passwords than it is to obtain physical tokens or biometrics.

Obtaining and Cracking Password Hashes

A "clear text password" is what a user would type when prompted to log in to a system. To avoid exposing a sensitive password, Microsoft AD stores user passwords in a secure, unintelligible

[4] Executive Order No. 14028, *Improving the Nation's Cybersecurity*, issued May 12, 2021, available at https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity. Our report represents a snapshot in time and describes conditions present during our fieldwork, which took place in February 2021. We provide additional detail in Appendix 1, which contains our scope and methodology. As described at the outset of this report, we provided this information to the Department promptly to ensure that it was able to implement appropriate corrective measures. We also note that, since the time of our fieldwork, the OMB published newer mandates with extended deadlines; we do not discuss those mandates or deadlines in this report because they are out of scope.

[5] Additional identification and authentication servicers, such as local, isolated systems that individual bureaus or offices may operate, were not in the scope of our inspection.

[6] NIST SP 800–63, *Digital Identity Guidelines*, issued June 2017, available at https://pages.nist.gov/800-63-3/.

format called "hashes."[7] The hashed version of a password is not usually accepted through typical authentication operations, such as computer login prompts. This restriction prevents a malicious actor from using captured password hashes to gain unauthorized access to a computer system.[8]

Clear Text Password vs. Hashed Password Examples

Clear Text Password*	=	`Password-1234`
Hashed Password†	=	`A71FB31235347EA75956B6155ED36899`

* This password is compliant with the Department's current password complexity requirements.

† This is the exact hash that represents `Password-1234` in Microsoft AD.

Hashes are generally considered secure because they cannot be directly reverted back to clear text—their original state. However, there are indirect methods attackers can use to attempt to recover hashed passwords. Accordingly, attackers seek to obtain password hashes in many different ways. For example, in our recent evaluation of the Department's wireless network security, we used an evil twin attack, a well-known technique to obtain clear text as well as hashed passwords.[9] Moreover, attackers can infect computers with malware, which can extract password hashes from the memory of the affected computer.

Once attackers have captured hashes, they must attempt to recover its original clear text form through a process referred to as "hash cracking." If successful, this enables the attacker to use the password to gain unauthorized access to an organization's computer systems and data. "Hash cracking" is the automated process of generating clear text password "candidates"[10] and then computing hashes of those candidates and comparing the results against captured hashes. If the candidate's hash matches the captured hash, it means the password candidate and the clear text version of the captured hash are the same. If the two hashes do not match, the process continues until either a match is found or the attacker gives up and attempts to crack other captured password hashes.

One method of cracking captured password hashes is a "brute force" attack, which is a technique in which every possible password candidate is generated and compared to the captured hash. Depending on the hash-cracking algorithm used and the complexity of the clear text password, a brute force attack can require a significant amount of time and computer resources to run through

[7] Stored or transmitted passwords are often hashed using one-way mathematical algorithms. Specifically, the algorithm converts a clear text password into a unique string of characters that cannot be directly reverted back to the clear text password.

[8] Some systems are vulnerable to the "pass-the-hash" hacking technique where attackers can use uncracked hashes to access systems (https://attack.mitre.org/techniques/T1550/002/). This vulnerability was out of scope for this project.

[9] As part of past penetration tests, we collected employee password hashes, cracked a high percentage of them (between 20 and 40 percent), and used the passwords to authenticate to systems and networks within the Department.
Report No. 2018–ITA–020, *Evil Twins, Eavesdropping, and Password Cracking: How the Office of Inspector General Successfully Attacked the U.S. Department of the Interior's Wireless Networks*, issued September 2020.
https://www.doioig.gov/sites/default/files/2021-migration/FinalAudit_WirelessNetworkSecurity_Public.pdf.

[10] Potential passwords being tested to determine if they match the hashed passwords are referred to as "candidates" in our tools.

every possible password candidate. For example, a brute force attack against a password hash that meets the Department's minimum password complexity requirements is estimated to take at least 136 years with a commercial off-the-shelf "hash-cracking system." Any password that exceeds these password complexity rules could take a millennium or more to crack.

Relying on brute force statistics only, however, may lead to a false sense of security because, with planning and dedicated hardware, password candidates may be generated with a much higher probability of success. For less than $15,000, we built a system designed specifically to crack password hashes using open-source software and a custom wordlist made up of dictionaries from multiple languages, U.S. Government terminology, pop culture references, and publicly available password lists harvested from past data breaches across public and private sectors. We created a set of rules and processes for manipulating and combining those words into password candidates. This process will not crack all password hashes acquired but, as discussed below, is likely to crack password hashes at a much higher rate than a brute force attack.[11]

The Department provided us with the hashes for every Department user account, which it organizationally divided by the following domains (these domains generally coincide with the Department's bureaus and offices):

- Bureau of Indian Affairs (BIA)
- Bureau of Land Management (BLM)
- Bureau of Reclamation (BOR)
- Bureau of Trust Funds Administration (BTFA)
- Departmental Offices, which the Department referred to as "DOI" in the data it provided[12]
- Interior Business Center (IBC)
- Minerals Management Service (MMS),[13] which covers the following bureaus and offices in the data the Department provided:
    - Bureau of Ocean Energy Management (BOEM)

[11] See Appendix 1 for our scope and methodology and details about how we configured our tests to be faster and more effective than a brute force attack alone.

[12] The Department AD system's structure does not directly follow the Department's overall organizational structure. Within the AD, the DOI domain contains most but not all of the Department's offices (see https://www.doi.gov/bureaus/offices for a list of the Department's offices). Some of the Department's offices have their own domain as identified in this list. For this report we use the same naming conventions to align with the Department's AD infrastructure.

[13] In 2010, the MMS was divided into three separate bureaus. The Department did not separate the AD infrastructure to represent these individual bureaus; instead, the Department continues to use the MMS domain to represent a combination of the three. For this report we use the same naming convention to align with the Department's AD infrastructure.

    - Bureau of Safety and Environmental Enforcement (BSEE)
    - Office of Natural Resources Revenue (ONRR)
- National Park Service (NPS)
- Office of Inspector General (OIG)
- Office of Surface Mining Reclamation and Enforcement (OSMRE)
- U.S. Fish and Wildlife Service (FWS)
- U.S. Geological Survey (USGS)

We attempted to crack all of the Department's user accounts as provided, but we have limited our reporting focus on this point to only the active user accounts. Because disabled accounts are not capable of authenticating to the AD, they present a lower risk of opportunity to compromise or exploit.

As part of our rules of engagement with the Department, we waited 90 days to begin testing hashes from the Department. At that time, all accounts should have had their passwords changed or been disabled due to inactivity pursuant to departmental policy. As of June 8, 2021, we provided the Department with a list of all user accounts with passwords we cracked to ensure that the Department forced those accounts to change passwords.

Password Lists Available on the Internet

We note that obtaining hashes and attempting to crack them is not always necessary, as there are a variety of other frequently used methods of obtaining passwords.[14] Additionally, lists of passwords obtained by previous breaches are readily available on the internet. In 2009, a company named RockYou was breached, exposing more than 14 million social media passwords.[15] In 2021, a new wordlist (named "RockYou2021") was published; the list contained not only compromised passwords but a compilation of words from multiple dictionaries and websites.[16] As noted previously, we used a similarly compiled list of breached passwords in combination with dictionary words in our hash-cracking system. As with password lists, there are also databases of previously cracked hashes readily available on the internet.

[14] For example, social engineering techniques, such as phishing scams, are one of the most common ways a password can be exposed.

[15] Cubrilovic, Nik. "RockYou Hack: From Bad to Worse." *TechCrunch*, December 15, 2009. https://techcrunch.com/2009/12/14/rockyou-hack-security-myspace-facebook-passwords/.

[16] The name of this new wordlist was misleading and widely, but incorrectly, reported as a new breach. The author of this wordlist includes a summary of all the sources they used at https://github.com/ohmybahgosh/RockYou2021.txt.

Authentication Requirements Continue To Evolve

Even if a password is compromised, MFA is a highly effective method of protecting accounts. It is not a new technology; various forms of MFA have been in use as an industry best practice[17] in the private sector for 35 years. MFA is also not a new requirement for Federal information systems—the Government first mandated MFA through the use of PIV cards for authenticating to information systems in August 2004.[18] NIST followed suit, and, in December 2006, it included MFA as a recommendation in its first revision of SP 800–53.[19] Since then, every revision of this document has continued to include MFA guidance, and the Department copies it as a requirement into its Security Control Standards as overarching cybersecurity policy.[20]

In June 2017, NIST published updated guidance for account and password management in its four-volume SP 800–63 document suite. This new guidance not only highlights weaknesses in password complexity requirements but strongly recommends that organizations implement MFA on all their computer systems instead of using passwords. Most recently, as noted previously, Executive Order No. 14028 mandated the widespread implementation of MFA by September 2021.

NIST has acknowledged that there may be cases where MFA is not yet possible and has published recommendations on how agencies can strengthen password complexity requirements in these cases. Specifically, NIST SP 800–63 recommends using passphrases instead of passwords; in addition, it directs agencies to implement controls to prevent users from creating new passwords that are commonly used, expected, or compromised.

Password vs. Passphrase Examples

Password	=	5pr1ng*Ish3re
Passphrase	=	DinosaurLetterTrailChance

NIST takes an updated approach to creating passphrases based on extensive research on human thought processes related to password creation and maintenance. NIST SP 800–63 discusses establishing password length requirements using a risk-based approach to determine the most effective minimum password length. In addition, NIST notes that an effective passphrase should not have a maximum limit. In 2017, the Director of NIST's Trusted Identities Group published an introduction to the new guidance. He noted that, over time, we have come to rely more and more on passwords in our daily lives, but bad actors have become steadily more efficient in defeating those passwords. This has resulted in a "negative feedback loop": as password policies imposed

[17] According to NIST, an industry best practice is "a procedure that has been shown by research and experience to produce optimal results and that is established or proposed as a standard suitable for widespread adoption." https://csrc.nist.gov/glossary/term/best_practice.

[18] See Homeland Security Presidential Directive No. 12: *Policy for a Common Identification Standard for Federal Employees and Contractors* (HSPD–12), issued August 27, 2004. https://www.dhs.gov/homeland-security-presidential-directive-12.

[19] NIST SP 800–53, Revision 1, *Recommended Security Controls for Federal Information Systems*, issued December 2006. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-53r1.pdf.

[20] The most recent revision, NIST SP–800–53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, was published in September 2020. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final.

more complexity requirements to slow down attackers, these same requirements made remembering passwords more difficult, leading users to turn to simple, easy-to-remember patterns. These common patterns, though, became an easy target for attackers, leading to additional password complexity requirements in a never-ending cycle.[21]

NIST SP 800–63 explains that if agencies implement longer passwords through the use of passphrases, the additional complexity requirements of mixing and matching characters (e.g., uppercase, lowercase, special) become less necessary because of the added difficulty of cracking the password hash of a lengthy phrase versus that of a single word. The enhanced security provided by using these longer passphrases also allows for less frequent password changes due to the lower risk of compromise. Randomized passwords that appear to be complex are often hard for users to remember but easy for a computer to crack. In contrast, lengthy, yet simple passphrases are much easier for a human to remember and are not as susceptible to hash-cracking methods such as brute force attacks.

[21] Garcia, Mike. "Easy Ways to Build a Better P@$5w0rd." *Taking Measure* (blog), NIST. October 4, 2017. https://www.nist.gov/blogs/taking-measure/easy-ways-build-better-p5w0rd.

Results of Inspection

We found that the Department's management practices and password complexity requirements were not sufficient to prevent potential unauthorized access to its systems and data. Notwithstanding the requirements of Executive Order No. 14028, *Improving the Nation's Cybersecurity*, the Department did not consistently implement MFA on its systems—most importantly, it did not implement MFA on 89 percent (25 of 28)[22] of its High Value Assets (HVAs).[23] A breach of an HVA has the potential to severely impact agency operations and result in the loss of sensitive data.

We cracked

18,174

of the Department's AD **user accounts**, which included

288

accounts with **elevated privileges** and

362

senior Government employee accounts.

In addition, the Department's password complexity requirements allowed passwords that we were able to crack relatively quickly. In particular, in the first 90 minutes of testing, our hash-cracking system obtained clear text passwords for 13,924 (16 percent) of 85,944 Department Active Directory (AD) user accounts. Overall, we cracked 18,174 (21 percent) of the Department's AD user accounts. We also cracked 288 passwords for accounts with elevated privileges and 362 passwords belonging to senior Government employees (GS–15 or higher, including senior executives)—among them, passwords belonging to 3 high-level OCIO management accounts and a total of 54 senior executives Departmentwide.

We also learned that the Department's password complexity requirements implicitly allowed unrelated staff to use the same inherently weak passwords and that the Department did not timely disable inactive accounts or enforce password age limits. It is likely that if a well-resourced attacker were to capture Department AD password hashes, the attacker would have achieved a success rate similar to ours in cracking the hashes. The significance of our findings regarding the Department's poor password management is magnified given our high success rate cracking password hashes, the large number of elevated privilege and senior Government employee passwords we cracked, and the fact that most of the Department's HVAs did not employ MFA.

The Department Did Not Consistently Implement MFA on Its Systems

We found that the Department allowed single-factor authentication (username and password) on an indeterminate number of its applications, notwithstanding 18 years of mandates from sources

[22] In November 2021, the OCIO could not validate the MFA status of all systems it reported to the OMB. We informed the OCIO that we would report on the HVA numbers based on information we had as of November 2021.

[23] According to the Cybersecurity and Infrastructure Security Agency, an HVA "is information or an information system that is so critical to an organization that the loss or corruption of this information or loss of access to the system would have serious impact to the organization's ability to perform its mission or conduct business." https://www.cisa.gov/sites/default/files/publications/CISAInsights-Cyber-SecureHighValueAssets_S508C.pdf.

including NIST, the U.S. Department of Homeland Security, and Executive Orders, as well as the Department's own internal policies. The Federal Information Security Modernization Act, or FISMA, requires the Office of Management and Budget (OMB) to submit annual reports on behalf of all executive Government agencies.[24] These reports included the total number of systems that were and were not enforcing MFA. We asked the OCIO for an inventory of applications enforcing MFA, and, although it provided us with the numbers it reported to the OMB, the OCIO was not able to identify the systems. This is because the OCIO relied on the bureaus and offices to self-report only the total numbers of systems that met the MFA requirement. The OCIO did not request enough information to identify individual systems, which would allow it to validate the bureau and office responses.

In addition, the Department did not track enforcement of MFA for HVA systems even though individual system owners are required to track the lack of MFA implementation in their Plans of Action and Milestones (POA&Ms).[25] Through a manual review of each HVA system, we determined that 89 percent (25 of 28) of the Department's HVAs do not require MFA. When we provided the Department with the data to support this finding, it was unable to confirm the MFA implementation status for the 25 systems, and we identified 14 systems with open POA&Ms related to MFA. The documented reasons the Department provided for continuing to allow single-factor authentication included lack of resources, reliance on external systems, or unspecified "impact to end users."

During our inspection, we learned that the OCIO did not validate statements by system owner that the implementation of single sign-on (SSO) authentication alone was a satisfactory MFA implementation method for all types of systems. SSO relies on the user's workstation to enforce MFA through the use of a PIV card and PIN to authenticate to the desktop and then passes the authentication to the requesting application. When this automatic authentication does not work as expected,[26] applications can still be configured to bypass MFA and accept single-factor authentication for access. The Department's Safety Management Information System (SMIS)—an application that tracks employee personal health information related to workers compensation claims and COVID–19 vaccine status—is an example of a system that uses SSO authentication but allows MFA to be bypassed and continues to permit the use of single-factor authentication. In fact, we determined that SSO authentication to the SMIS is easily bypassed by using a browser that does not support SSO authentication on any client device regardless of whether SSO is enabled.

In these cases, bureau and office system owners reported that they met MFA implementation requirements through SSO in their official system documentation even though single-factor authentication was not disabled on those systems. Without an inventory from the OCIO accurately identifying the applications enforcing MFA, we were unable to test how many systems incorrectly relied on SSO to meet the Department's MFA requirements.

[24] Federal Information Security Modernization Act, Pub. L. No. 113–283, available at https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf.

[25] Federal systems are required to document all weaknesses in POA&M documents. These should include an analysis of the steps needed to mitigate the weaknesses, the cost, and scheduled completion dates. For additional information and a listing of relevant NIST and OMB requirements, see https://csrc.nist.gov/glossary/term/plan_of_action_and_milestones.

[26] Causes can include unsupported browsers, nonstandard workstations, or rogue devices.

We learned that the Department enforced MFA for 99 percent of user accounts with elevated privileges (4,016 of 4,062) through the Smart Card Required for Interactive Login (SCRIL) configuration option in its AD. If SCRIL is enabled on an account, the user is unable to use single-factor authentication on any system that relies on the Department's AD for authentication, even if that system supports single-factor authentication. Enforcing SCRIL for all users—rather than relying on SSO alone—is another way for the Department to meet MFA requirements. While SCRIL can resolve this issue across all applications, it can be difficult to implement across multiple platforms and devices.

One reason the Department did not widely use the SCRIL configuration is that it does not support non-PIV MFA (e.g., other types of hardware tokens or authenticator apps). The Department did not enable SCRIL on 94 percent of its accounts (80,740 of 85,944) because of this lack of support. For example, SCRIL currently breaks mobile device (i.e., phone or tablet) connectivity to the Department's Office 365 environment because mobile devices do not support PIV authentication without additional hardware and software. This means that the Department cannot use PIV authentication as its only MFA implementation because doing so would inhibit the use of mobile devices and tablets. Implementing derived credentials—certificates derived from PIV card authentication and approved by NIST—for mobile devices would make this setting possible for Office 365 on mobile devices.

The Department relied on authentication methods that were not in line with NIST recommendations, Governmentwide mandates, and industry best practices.[27] This placed the burden of the Department's security controls on obsolete password complexity requirements, as discussed in more detail below. Further, the Department did not have a full picture of which systems complied with which standards. If it does not require and enforce MFA across its systems—including those that contain sensitive information such as the SMIS—the Department's data remains at risk of unauthorized exposure.

Recommendations

We recommend that the Department:

1. Prioritize implementing PIV or other Department-approved MFA methods that cannot be bypassed to allow single-factor authentication for all applications, starting with the Department's HVAs.

2. Develop and implement a process to track and validate MFA status for all Department information systems.

[27] See Microsoft's "Azure Identity Management and access control security best practices" at https://docs.microsoft.com/en-us/azure/security/fundamentals/identity-management-best-practices.

The Department's Ineffective Password Complexity Requirements Allowed Easy-To-Crack Passwords

4.75 percent of all passwords for active accounts **used the word "password"** as a basis.

The Department's *Security Control Standard: Identification and Authentication* (Version 4.1, dated September 2016) requires that all passwords have a minimum length of 12 characters and contain at least 3 of 4 character types consisting of uppercase, lowercase, digits, and special characters. We found that these requirements were not sufficient to prevent us from successfully recovering the clear text passwords for 18,174 active user accounts (21 percent) using our hash-cracking system (see Figure 1). We recovered passwords for 13,924 of those accounts in the first 90 minutes of testing and recovered the passwords for the remaining 4,250 accounts over an additional 8 weeks of testing.

Figure 1: Summary of Cracked Hashes by Account Type

Account Type	No. of Accounts	No. Cracked	% Cracked
Individual	72,751	15,164	21
Senior	1,789	362	20
Elevated	4,062	288	7
Shared*	11,031	2,765	25
Service†	2,162	245	11
Total Accounts‡	**85,944**	**18,174**	**21%**

* Shared accounts are those used by two or more individuals, typically mailboxes.

† Service accounts are those used by computer system processes, not people.

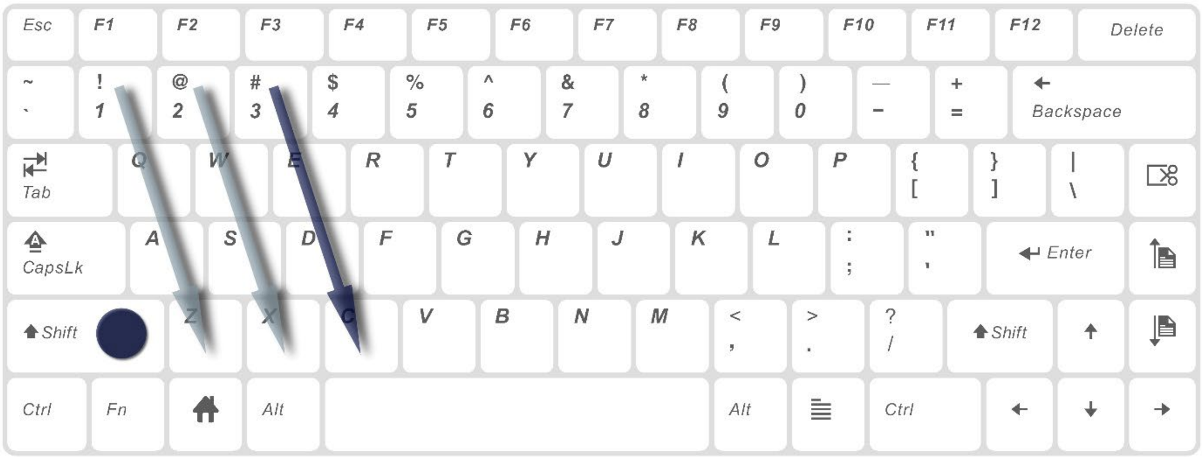
‡ Some account types overlap; those accounts are not duplicated in the totals.

We note that 99.99 percent of the accounts we cracked met the Department's password complexity requirements. These passwords, however, were consistently made up of single dictionary words, patterns, or slightly modified existing passwords—which people tend to use to construct memorable passwords (e.g., `Changeme$12345`, `Polar_bear65`, `Nationalparks2014!`). Although the Department's current requirements appear to encourage complex passwords, in practice, its policies were not sufficient to prevent users from creating passwords that are easy to crack. As discussed in more detail below, we also found many of the same passwords in use on user accounts across multiple bureaus and offices.

Easy-To-Crack Passwords

Most of the passwords we cracked were based on a single dictionary word with the inclusion of enough characters or character substitutions to meet the password complexity requirements. For example, `Password-1234` was the most used password at the Department. Even though a password of this type meets requirements because it includes uppercase, lowercase, digits, and a special character, it is extremely easy to crack. The second most frequently used password was `Br0nc0$2012`. Although this may appear to be a "stronger" password, it is, in practice, very weak because it is based on a single dictionary word with common character replacements. As stated earlier, NIST SP 800–63 recommends longer passphrases made up of multiple unrelated words because those are far more difficult for a computer to crack. Another deceptively weak type of password we found at the Department is one that uses a keyboard pattern. For example, the password `1qaz2wsx#EDC` may appear at first glance to be random, but it is simply a pattern using keys on a standard U.S. keyboard (see Figure 2).

Figure 2: Example of a Keyboard Pattern Password


Esc F1 F2 F3 F4 F5 F6 F7 F8 F9 F10 F11 F12 Delete
~ ` ! 1 @ 2 # 3 $ 4 % 5 ^ 6 & 7 * 8 (9) 0 — – + = Backspace
Tab Q W E R T Y U I O P { [}] | \
CapsLk A S D F G H J K L : ; " ' Enter
Shift Z X C V B N M < , > . ? / Shift
Ctrl Fn Alt Alt Ctrl

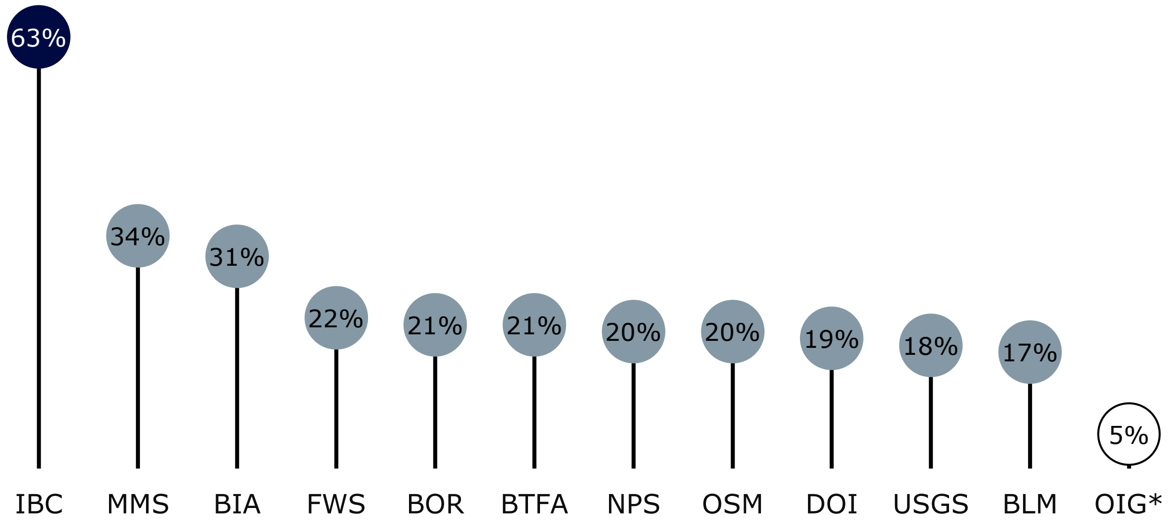
Potential password pattern: light blue arrows = `1qaz2wsx`, dark blue arrow indicating shift function = `#EDC`, combined password pattern = `1qaz2wsx#EDC`

Frequent password change requirements, while crucial when weak passwords are permitted, tend to encourage users to continue to use passwords that are easy to crack. NIST SP 800–63 states that when frequent password changes are required, users are most likely to change a single character, or append a character to the end of an existing password (e.g., `Password-1234` might become `Password-1234!`). This ensures that the password remains memorable to the user, but it also remains weak and easy to crack. Similarly, passwords derived from keyboard patterns tend to keep the same pattern but shift to new keys. This creates a feedback loop that frustrates users, perpetuates the weak password cycle, and does not improve security.

Bureau and Office Accounts

We found a wide variance when we broke down our results by bureau and office. We cracked approximately 20 percent of accounts at most bureaus and offices; however, we were able to crack 63 percent of the IBC's accounts and only 5 percent of our own OIG accounts[28] (see Figure 3).

Figure 3: Percent of Cracked Accounts at Each Bureau and Office



* See Footnote 28 for additional information on the OIG's status and inclusion in this report.

These variances occurred over multiple account types and would require significant additional research to determine the specific cause for each individual account's differences. The overarching cause for the variances was the decentralized implementation of departmental policy at the bureaus and offices and the lack of oversight within the Department's AD infrastructure. Ultimately, the OCIO is responsible for developing and updating policies that conform to the information security mandates such as those from NIST, the U.S. Department of Homeland Security, and the OMB. The OCIO is also responsible for ensuring that bureaus and offices comply with these policies.

[28] On this point, the OIG has a unique status within the Department. Pursuant to the Inspector General Act of 1978, we have specific authorities and the capacity (and obligation) to act independently on a range of issues, and we have dual reporting obligations to both the head of the Department and to Congress. We have also, however, made the decision to share infrastructure with the Department for compatibility and access to departmental data and resources. Because of the fact that we rely on some aspects of the Department's IT infrastructure, we considered the OIG's performance with respect to the issues we cover in this report. We initially tested our password cracking methodology against only the OIG domain. The OIG was in the process of researching products that could implement stricter controls on passwords at the time of our initial test. During this inspection, we noted a 35-percent reduction in cracked passwords between our first and second rounds of testing. See Appendix 1 for more information about our methodology.

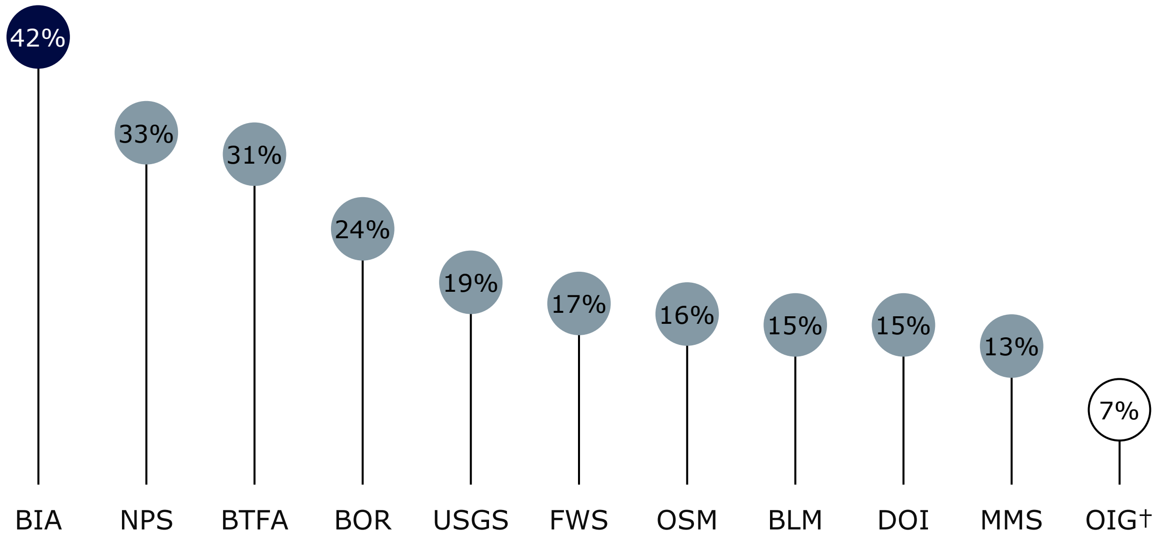
High-Risk and Senior Government Employee Accounts

We also found that bureaus and offices did not prioritize security on all high-risk accounts. Accounts belonging to senior Government employees or those with elevated privileges present a higher risk because of the additional access granted to potentially sensitive information or the ability to make changes to systems or networks. In addition, malicious actors frequently target accounts belonging to people in positions of authority.

While the Department enabled SCRIL on 99 percent of accounts with elevated privileges, it did not implement additional security measures for accounts belonging to senior Government employees because the Department incorrectly believed its password complexity rules were sufficient to secure the accounts from compromise. These high-risk accounts had nearly the same conditions as those we found across the testing universe.

Nearly every elevated account we cracked was protected by SCRIL, but none of the senior Government employee accounts we cracked had this setting enabled. Overall, we cracked the passwords for 20 percent of the Department's senior Government employee accounts, including 3 high-level OCIO management accounts and 54 senior executives Departmentwide (see Figure 4).

Figure 4: Percent of Cracked Senior Government Employee Accounts at Each Bureau and Office*



* The IBC domain did not contain accounts belonging to senior Government employees and is not represented in this figure.

† See Footnote 28 for additional information on the OIG's status and inclusion in this report.

Recommendations

We recommend that the Department:

3. Revise password complexity and account management policies to reflect the updated risk-based approach set forth in the NIST SP 800–63 document suite, such as using longer passphrases and less frequent change intervals.

4. Implement controls to monitor, limit, or prevent commonly used, expected, or compromised passphrases and passwords in accordance with NIST SP 800–63 and NIST SP 800–53.

5. Prioritize the inventory, monitoring, and enforcement of existing controls as well as the controls we recommended in this report for accounts belonging to senior Government employees or accounts with elevated privileges.

The Department's Password Complexity Requirements Implicitly Allowed Hundreds of Unrelated Accounts To Use the Same Passwords

We found that the same easy-to-crack passwords (which all met the Department's complexity requirements as defined in its *Security Control Standard: Identification and Authentication*) were used across multiple active accounts.[29] Even though many of these accounts were unrelated to each other, the passwords were so common that multiple employees from different bureaus and offices independently chose the same passwords. Because the Department did not have an explicit rule in place denying this practice, it implicitly allowed users to create the same passwords across multiple accounts.[30] For example, 48 employees from the BLM, BOR, DOI, FWS, NPS, and USGS selected the password `Winter2021!!`. One of these user accounts belonged to a senior Government employee. Similarly, 16 employees from the BLM, BOR, MMS, FWS, NPS, and USGS selected the password `January2021!`. Moreover, the Department's 60-day password change requirement combined with its password complexity requirements again created a negative feedback loop that encouraged users to select weak passwords that were easy to remember.

In other cases, we found common passwords reused across multiple related accounts, such as new accounts with temporary passwords, shared mailboxes, or service accounts. Understanding

[29] The most commonly understood example of password reuse is when a single individual uses the same password for accounts across multiple systems (e.g., an online shopping account, a personal email account, and a media streaming account often using the same username). This approach can introduce additional risk, especially when the accounts are relatable through common identifying factors such as username or email. When one of those systems is breached and the user's password is leaked, the risk that the other accounts will be compromised rises significantly—this was one of the key factors reported in the Colonial Pipeline attack. This type of password reuse was not within the scope of our inspection. See Appendix 1 for additional details.

[30] An explicit rule is one in which the system specifies an action, such as permitting or denying a password, when presented with certain parameters. An implicit rule is when the system does not have a specified action in place and thus either implicitly permits or denies the request.

the purpose and extent of access granted to these accounts was out of the scope of our inspection; therefore, we were unable to identify the extent of the risk posed by these and other nonadministrative accounts. Service accounts are often granted elevated privileges over systems or data, and shared mailboxes often contain sensitive data or attachments.

We found that 20 percent of all active accounts had passwords that were used across multiple distinct accounts (16,812 out of 85,944). This includes both cracked and uncracked passwords. We were able to identify when the same passwords were used based on the hashes, so even if we did not crack a password, we could identify and determine which accounts shared the same password. Figure 5 shows the top 10 most used passwords that we cracked by bureau and office—half of which contained a combination of the word "password" and the sequence "1234." We also identified the number of accounts using these passwords for more than 60 days in violation of the current maximum password age policy or that have elevated privileges. The accounts with elevated privilege included one domain administrator account, which is the highest level of privileges.

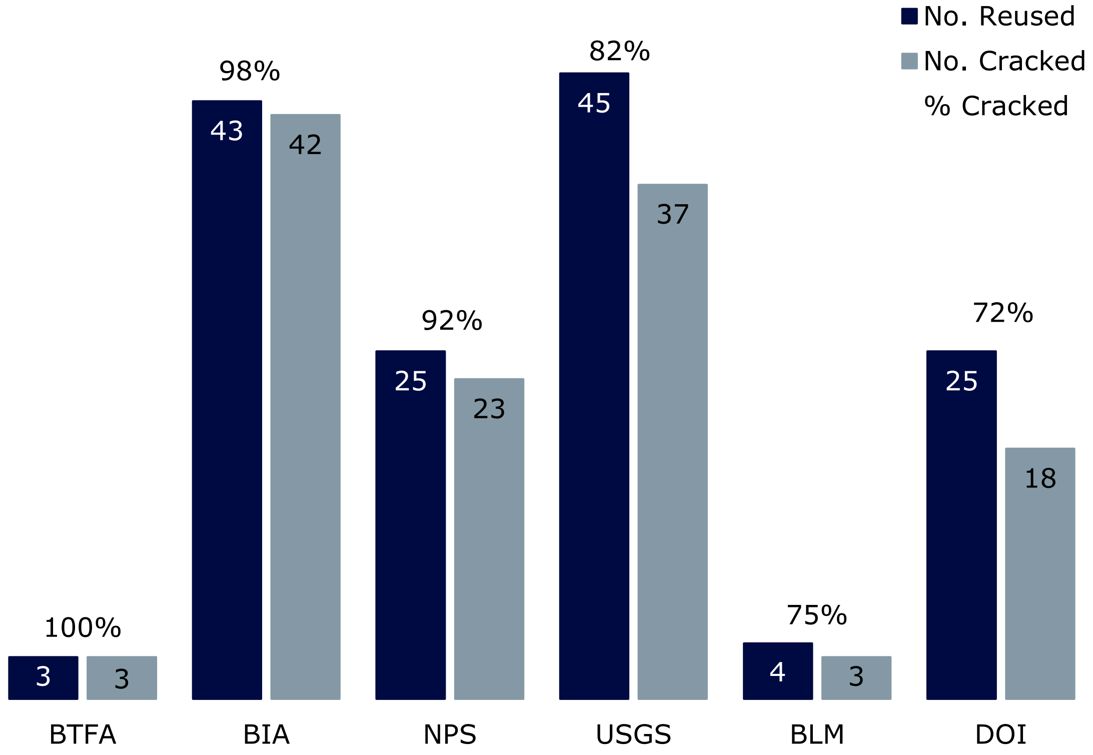
Figure 5: Top 10 Most Reused Passwords

Password	Bureau/Office	No. of Accounts	Violates Age Policy	Elevated Privileges
Password-1234	MMS	478	407	1
Br0nc0$2012	IBC, DOI	389	374	0
Password123$	NPS, BIA, FWS, USGS	318	0	2
Password1234	NPS, BIA, FWS, BOR, MMS, BTFA	274	44	3
Summ3rSun2020!	NPS	191	0	0
0rlando_0000	USGS	160	158	1*
Password1234!	NPS, BIA, FWS, USGS, BLM, MMS, DOI, BTFA	150	1	2
ChangeIt123	FWS	140	0	0
1234password$	BIA	138	0	3
ChangeItN0w!	FWS	130	0	0

* This password was used on a domain administrator account with the highest level of privileges.

Additionally, we found that accounts with elevated privileges and those of senior Government employees at five bureaus and within the DOI domain were among the unrelated accounts using the same passwords. We cracked senior Government employee accounts that used the same passwords at the Department level, and at the BIA, BTFA, NPS, USGS, and BLM (see Figure 6).

Figure 6: Cracked Senior Government Employee Accounts Using the Same Passwords



Password reuse is a security risk because it reduces both the time and effort necessary for a successful attack. The risk is greatly increased when the same easy-to-crack passwords are allowed to be used on multiple accounts.

A common attack against password reuse is called password spraying, which is when attackers use automated tools to test many accounts with just a few known passwords.[31] In 2021, it was reported that the same hackers who breached SolarWinds successfully in 2020 used password spraying against Microsoft.[32] Two of the top ten reused passwords at the Department (`Password-1234` and `Password123!`) can be found in breached password lists available on the internet. A password spraying attack using those two passwords would have been successful on a total of 628 active accounts, 3 of which had administrative privileges. Our findings demonstrate how password spraying attacks are especially successful when known passwords are reused on high-risk accounts such as those with elevated privileges or access to sensitive information.

NIST SP 800–63 requires agencies to check potential passwords and disallow them if they are on a list of commonly used, expected, or compromised passwords. We found that none of the

[31] Kelley, Diana. "Protecting your organization against password spray attacks." *Microsoft Security* (blog). Microsoft. April 23, 2020. https://www.microsoft.com/security/blog/2020/04/23/protecting-organization-password-spray-attacks/.

[32] Goodin, Dan. "SolarWinds hackers breach new victims, including a Microsoft support agent." *Ars Technica*. June 26, 2021. https://arstechnica.com/gadgets/2021/06/solarwinds-hackers-breach-new-victims-including-a-microsoft-support-agent/.

Department's bureaus had implemented the ability to check for and prevent weak passwords.[33] These weaknesses should be addressed to minimize risk to the Department and its systems. As we note in the "Background" section, we took steps to ensure that the Department was promptly made aware of the vulnerabilities we identified and that it had the opportunity to remedy those vulnerabilities to the extent possible. The recommendations we have included throughout this report, if implemented, will assist the Department in addressing these concerns systematically.

Recommendations

We recommend that the Department:

6. Revise account management policy to prohibit related accounts from using the same passphrases and passwords (e.g., shared mailboxes, service accounts, or users with multiple service-level accounts).
7. Implement guidance requiring temporary passphrases and passwords to be unique and complex, rather than using a common variation or reusing the same passphrase or password.

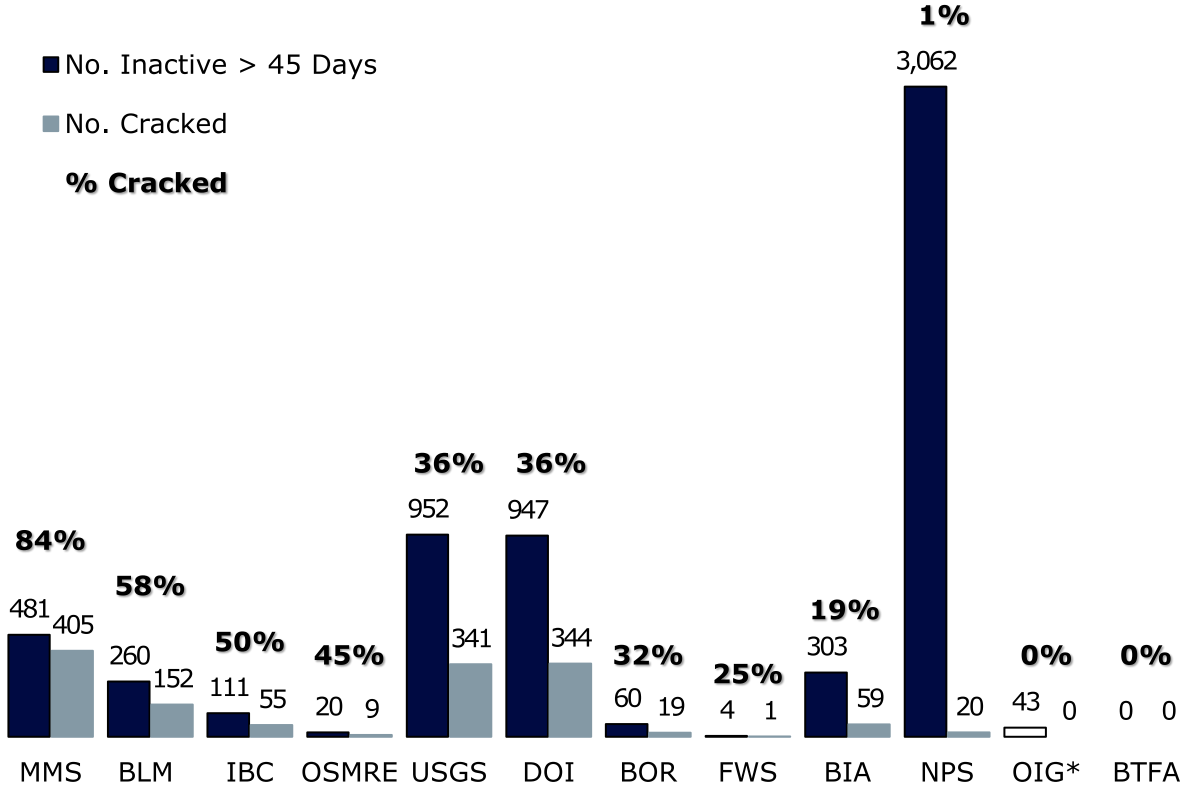
The Department Did Not Timely Disable Inactive Accounts or Enforce Password Age Limits

We found that the Department failed to enforce its own account management policies regarding account disabling and password changes as defined in *Security Control Standard: Access Control* (Version 4.1, dated September 2016) on a significant number of accounts. The Department's policy requires accounts to be disabled after 45 days of inactivity. Enforcing this provision is important because unused accounts pose a higher risk to Department systems and networks because they offer more opportunities for a malicious actor to gain unauthorized access. Disabling accounts after a period of inactivity reduces this risk because more accounts provide more opportunities for attackers.

[33] The OIG recently implemented a product that prevents accounts from using common dictionary words and previously compromised passwords. For example, if a user attempts to set a password that is on the restricted list, the system will notify the user that the selection is not allowed and prompt him or her to choose a different password.

We found that 6,243 of all active accounts had not been used for more than 45 days (see Figure 7); the Department failed to disable these accounts per its own policy and instead left implementation and enforcement of this policy to the bureaus and offices. We cracked 23 percent (1,405) of these accounts.

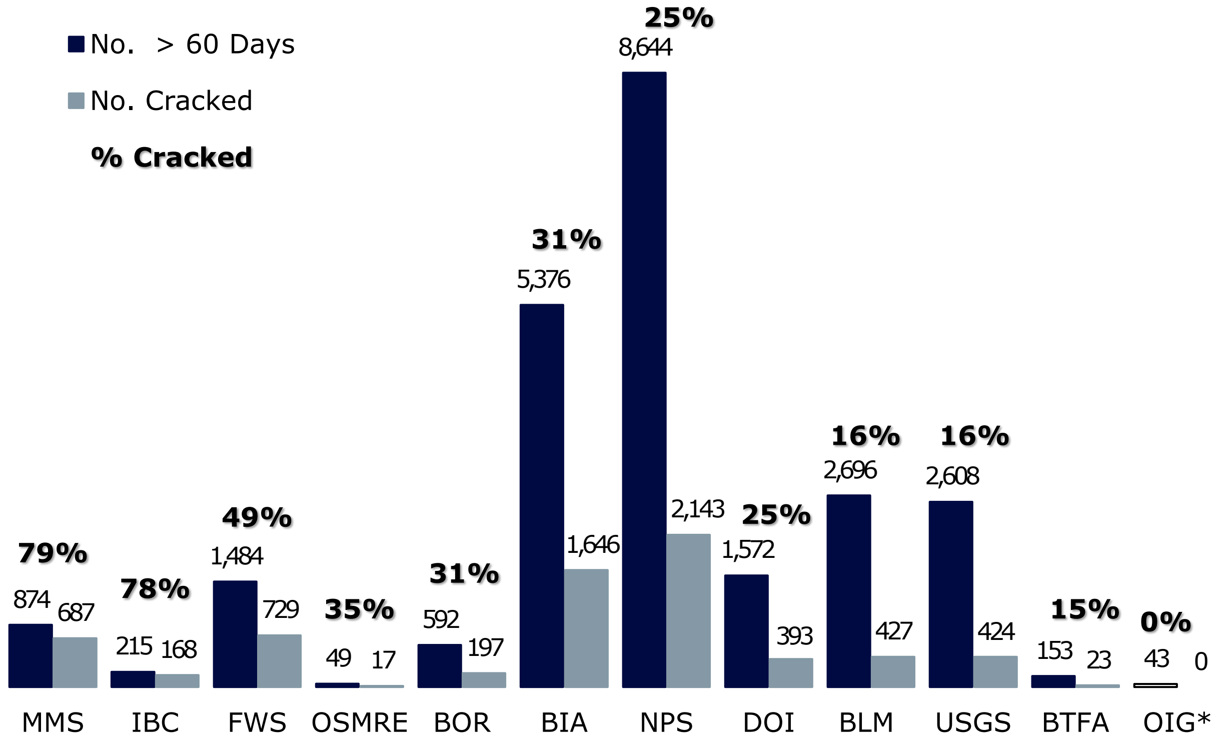
Figure 7: Cracked Accounts That Were Inactive More Than 45 Days



* See Footnote 28 for additional information on the OIG’s status and inclusion in this report.

We also found that 28 percent of the accounts we cracked did not comply with the Department policy requiring password changes at 60-day intervals, suggesting that these accounts were still using the passwords after we cracked them[34] (see Figure 8). Without that password age limit, an attacker is not limited by time. According to current Department policy, an attacker would have only 60 days to intercept or otherwise acquire a hash, crack it, and then use it. Frequent password changes combined with the Department's password complexity requirements created a negative feedback loop that encouraged users to select weak passwords that were easy to remember; however, enforcing the password age limit reduces the timeframe to exploit these weaknesses. This feedback loop can be eliminated with the implementation of MFA and passphrases, which in turn allows for longer password change intervals.

Figure 8: Cracked Accounts With Passwords Older Than 60 Days



* See Footnote 28 for additional information on the OIG's status and inclusion in this report.

These accounts had the same complexity requirements as the rest of the Department, and, as such, were weak and easy to crack. Department systems and accounts are critically at risk when outdated complexity requirements are combined with infrequent password changes.

[34] As described in Appendix 1, we waited 90 days after receiving the password hashes before beginning our testing. This was to ensure that any passwords we cracked would have been changed and unusable at the time of our testing.

Recommendation

We recommend that the Department:

8. Establish procedures and accountability mechanisms to ensure compliance with policies regarding account management monitoring and timely disabling of inactive accounts.

Conclusion and Recommendations

Conclusion

In the current cyberthreat environment, strong authentication methods and robust account and password management practices are necessary to help protect computer systems from unauthorized access. Overreliance on passwords to restrict system access to authorized personnel can have catastrophic consequences. For example, in 2021, *Forbes* reported that cybercriminals launched a ransomware attack on the Colonial Pipeline—"effectively shutting down half of the country's fuel supply chain—by stealing one password." The attack affected millions of businesses and consumers, and the White House declared a state of emergency.

The Colonial Pipeline ransomware attack is an example of the potential consequences of lack of multifactor authentication and weak account management practices. We did not attempt to compromise the Department's network by exploiting the vulnerabilities we found because such testing was out of scope. While a breach to the Department's computer network could have a significant adverse effect on its operations, such a breach would not produce the same widespread disruption to businesses and consumers that resulted from the Colonial Pipeline IT security incident. That being said, the cyberattack against the Colonial Pipeline reportedly succeeded because of a combination of weak IT security practices. At the Department, we found several of the same IT security weaknesses that enabled the successful cyberattack that was reported to have shut down operations on the Colonial Pipeline. Specifically, notwithstanding 18 years of requirements, the Department did not implement MFA on 89 percent of its HVAs. Moreover, the Department allowed employees to reuse passwords across multiple accounts and did not timely disable inactive accounts. Outdated authentication methodologies and password policies can lead to a higher risk of compromised accounts. When these compromises occur with senior Government employees or users with elevated privileges the impact can be significantly compounded because of the level of access to information and systems.

When MFA is implemented correctly, it adds a layer of security that protects organizations—even when passwords are compromised. The Department, however, did not fully implement MFA requirements that have been in place for more than 15 years. In addition, when we asked the Department to provide a detailed status of MFA across the agency, it told us that information did not exist. This failure to prioritize a fundamental security control led to continued use of single-factor authentication.

We found that the Department's management practices and password complexity requirements were not sufficient to protect against potential unauthorized access. We cracked passwords for 21 percent of all active accounts across the Department because its complexity requirements allowed users to make weak passwords. Our test results illustrated NIST's conclusion that forcing complex password composition rules will result in predictable password patterns. NIST also concluded that overly complex passwords become difficult for users to remember, so they are at a higher risk of being stored in an unsafe manner. The Department's reliance on single-factor authentication only increased the importance of aligning its account management requirements with NIST's recommendations.

Our findings demonstrate that the OCIO did not validate that the bureaus and offices were implementing effective controls to meet required password policies. The Department's lack of enforcement of its current account management policies is a risk multiplier when combined with single-factor authentication. Disabling access for accounts that have been inactive for long periods of time is a standard practice to mitigate the risk of potentially weak passwords being cracked. Ultimately, single-factor authentication is the highest risk configuration option for system and application access. To best mitigate the risk of easy-to-crack passwords, the Department must prioritize MFA on all systems and applications.

We make eight recommendations to help the Department strengthen its IT security by improving user account management practices.

Recommendations Summary

We provided a draft of this report to the Department for review and updated our final report to incorporate clarifying language and relevant facts. These updates did not change our findings or recommendations based on the evidence and controls as tested. We note that the Department commented, "[t]his report fundamentally asserts that passwords as lone credentials for authentication are not sufficient for modern information systems. The Department agrees." The Department concurred with all eight of our recommendations. We consider Recommendations 1–4 and 6–8 resolved but not implemented and Recommendation 5 unresolved. Below we summarize the Department's response to our recommendations, as well as our comments on its response. See Appendix 2 for the full text of the Department's response; Appendix 3 lists the status of each recommendation.

We recommend that the Department:

1. Prioritize implementing PIV or other Department-approved MFA methods that cannot be bypassed to allow single-factor authentication for all applications, starting with the Department's HVAs.

   Department Response: The Department concurred with the recommendation and stated that it is "working to meet the MFA requirements" in Executive Order No. 14028 and the OMB's January 2022 Memorandum M–22–09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*. The Department stated that it issued a Zero Trust Strategy and OCIO Memorandum, *Implementation of Multi-Factor Authentication using Phishing-Resistant Credentials Direct*ive, on August 26, 2022, that "directs all bureaus and offices to enforce MFA through the Department's approved phishing-resistant MFA services for all information systems and establishes prioritization of Department-approved MFA methods across the agency." The Department further stated that it would "take a risk-based approach in prioritizing the conversion of systems and applications from legacy authentication methods to MFA." The Department provided a target implementation date of December 30, 2024.

OIG Comment: Based on the Department's response, we consider Recommendation 1 resolved but not implemented. Although the target completion date is approximately 2 years from this report's issuance date, we acknowledge that it is within the timeframe noted in the latest mandate the OMB published after we completed our fieldwork.

2. Develop and implement a process to track and validate MFA status for all Department information systems.

   Department Response: The Department concurred with the recommendation and stated that its August 26, 2022 memorandum requires all bureaus and offices to enforce MFA for all information systems no later than the end of FY 2025. The Department stated that the OCIO will "develop a process to track compliance with this memorandum." The Department provided a target implementation date of April 30, 2023.

   OIG Comment: Based on the Department's response, we consider Recommendation 2 resolved but not implemented.

3. Revise password complexity and account management policies to reflect the updated risk-based approach set forth in the NIST SP 800–63 document suite, such as using longer passphrases and less frequent change intervals.

   Department Response: The Department concurred with the recommendation and stated that it is revising its Security and Privacy Control Standards to adopt the NIST SP–63 recommendations as specified in M–22–09. It further stated that new policies will take effect upon issuance of these standards. The Department provided a target implementation date of January 26, 2023.

   OIG Comment: Based on the Department's response, we consider Recommendation 3 resolved but not implemented.

4. Implement controls to monitor, limit, or prevent commonly used, expected, or compromised passphrases and passwords in accordance with NIST SP 800–63 and NIST SP 800–53.

   Department Response: The Department concurred with the recommendation and stated that it will implement Azure AD Password Protection for the AD accounts the OCIO manages. The Department provided a target implementation date of March 31, 2024.

   OIG Comment: The target implementation date for this recommendation is more than 1 year from this report's issuance date. This proposed timeframe is of concern to our office because monitoring of controls is essential to ensuring conformity with policies and regulations. The Department should revise its target implementation date and provide the revised date to the Office of Policy, Management and Budget (PMB). If the revised date is more than 90 days from this report's issuance date, the Department should establish mitigating measures until the recommendation is fully implemented. Based on the Department's response, we consider Recommendation 4 resolved but not implemented.

5. Prioritize the inventory, monitoring, and enforcement of existing controls as well as the controls we recommended in this report for accounts belonging to senior Government employees or accounts with elevated privileges.

   Department Response: The Department concurred with the recommendation and stated that it "already prioritizes the monitoring and enforcement of controls for accounts handling sensitive information and/or privilege access." The Department also said, "For the tested domain, DOI.Net, domain administrative accounts are very restrictive and monitored closely. Server administrators are less restrictive; therefore, the Department has inventory and monitoring for their identity activity."

   OIG Comment: We acknowledge in the report the higher level of effort the Department has put into protecting higher level administrative accounts. However, during our review, we found that the additional controls were either not implemented or ineffective, evidenced by the fact that we cracked 288 passwords for accounts with elevated privileges and 362 passwords belonging to senior Government employees. Therefore, the recommendation will remain unimplemented until the Department provides documentation demonstrating that it has prioritized the inventory, monitoring, and enforcement of existing controls belonging to senior Government employees or accounts with elevated privileges. Based on the Department's response, we consider Recommendation 5 unresolved.

6. Revise account management policy to prohibit related accounts from using the same passphrases and passwords (e.g., shared mailboxes, service accounts, or users with multiple service-level accounts).

   Department Response: The Department concurred with the recommendation and stated that it will revise its policy "to manage risk posed by re-use of passwords across multiple system accounts." The Department provided a target implementation date of January 26, 2024.

   OIG Comment: The target implementation date for this recommendation is more than 1 year from this report's issuance date. This proposed timeframe is of concern to our office because enforcing controls is essential to ensuring conformity with policies and regulations. The Department should revise its target implementation date and provide the revised date to the PMB. If the revised date is more than 90 days from this report's issuance date, the Department should establish mitigating measures until the recommendation is fully implemented. Based on the Department's response, we consider Recommendation 6 resolved but not implemented.

7. Implement guidance requiring temporary passphrases and passwords to be unique and complex, rather than using a common variation or reusing the same passphrase or password.

   Department Response: The Department concurred with the recommendation and stated that it has drafted new password complexity and length policies. The Department noted that the "OCIO will review this draft policy in light of this recommendation and ensure that our policies meet M–22–09." The Department provided a target implementation date of May 1, 2023.

   OIG Comment: Based on the Department's response, we consider Recommendation 7 resolved but not implemented.

8. Establish procedures and accountability mechanisms to ensure compliance with policies regarding account management monitoring and timely disabling of inactive accounts.

   Department Response: The Department concurred with the recommendation and stated that the "OCIO has existing procedures and mechanisms to implement policies regarding disabling of inactive accounts. . . . The OCIO and other relevant program offices will work with bureaus and offices to ensure that practices are consistently implemented to ensure accounts that need to be disabled are flagged in a timely manner." The Department provided a target implementation date of January 26, 2024.

   OIG Comment: The target implementation date for this recommendation is more than 1 year from this report's issuance date. This proposed timeframe is of concern to our office because monitoring of controls is essential to ensuring conformity with policies and regulations. The Department should revise its target implementation date and provide the revised date to the PMB. If the revised date is more than 90 days from this report's issuance date, the Department should establish mitigating measures until the recommendation is fully implemented. Based on the Department's response, we consider Recommendation 8 resolved but not implemented.

Appendix 1: Scope and Methodology

Scope

We performed our hash-cracking tests against all accounts contained in the U.S. Department of the Interior's Active Directory (AD), which included all of the Department's bureaus and offices. The scope of our project was limited to the Department's AD infrastructure, which provides centralized authentication to its systems. We did not evaluate passwords from systems operating their own authentication mechanisms, such as the Department's timekeeping or travel systems. We could not evaluate passwords used at third-party or partner organizations, such as vendors, contractors, or social media. Accordingly, our analysis and subsequent findings are also limited to only the accounts within the AD.

We coordinated with the Department's Office of the Chief Information Officer (OCIO) to validate our scope and methodology and define the rules of engagement[35] to minimize risk. In particular, our rules of engagement included a method for the Department to securely extract password hashes from its AD and transfer them to our IT Audits group for testing, including:

- Exporting the AD database, including the password hashes.
- Transferring the hashes and basic account information from the database to secure media.
- Waiting 90 days for passwords to expire before attempting to crack them.
- Keeping our systems offline.
- Destroying the original raw data from the Department after testing, while preserving the results and analysis that support our findings and recommendations.

Methodology

We conducted our inspection in accordance with the *Quality Standards for Inspection and Evaluation* as put forth by the Council of the Inspectors General on Integrity and Efficiency. We believe that the work performed provides a reasonable basis for our conclusions and recommendations.

During the research and development phase of this inspection, we performed initial testing of our methodology against only the Office of Inspector General (OIG) domain hashes. This allowed us to validate our processes and procedures for this larger scoped inspection. We reported our findings and recommendations to OIG management at the time of initial testing.

[35] According to the National Institute of Standards and Technology, rules of engagement define detailed guidelines and constraints regarding the execution of information security testing. The rules are established before the start of a security test and give the test team authority to conduct defined activities without the need for additional permissions. https://csrc.nist.gov/glossary/term/rules_of_engagement.

To accomplish our objective, we analyzed the data included in the AD account information (username, domain,[36] last log in, last password change, and other organizational data as provided), we conducted interviews, we issued data calls, we reviewed relevant criteria, and we performed four types of technical tests against the Department's AD hashes.

Test 1: Rules Plus Wordlist Attacks

Our password hash-cracking methodology started with a combination "rules plus wordlist" attack. This type of attack is the most efficient method of cracking passwords that are too long for a brute force attack. Wordlists in combination with rules to manipulate those words can generate password candidates with lengths well beyond the minimum 12 characters required by the Department.

We used a wordlist containing more than 1.5 billion words that included:

- Dictionaries from multiple languages.
- U.S. Government terminology.
- Pop culture references.
- Publicly available password lists harvested from past data breaches across both public and private sectors.
- Common keyboard patterns (e.g., "qwerty").

We tested this wordlist against approximately 30 million unique rules that convert each word in the list in various ways (e.g., changing letters to a visually similar digit or special character, switching capitalization, or prepending or appending additional digits or special characters). This means that we tested approximately 45 quadrillion password candidates against each hashed password.

Test 2: Mask Attacks

We performed additional, more time-consuming tests that involved testing common password patterns called "mask" attacks. A mask attack is a more focused type of brute force attack that tests a specific pattern (e.g., a mask can represent a password with the format: one capital letter followed by seven lower case letters, then four numbers, ending with one special character). Every possible combination that matches the mask is then tested as a password candidate. We analyzed passwords disclosed in past public breaches and identified 30 of the most common unique masks that comply with the Department's current password complexity requirements.

[36] The AD can organize the user accounts into what are known as domains; the OCIO has divided all bureau and office user accounts into domains that generally follow the Department's bureau and office organizational structure with some exceptions (e.g., the OIG is a standalone domain instead of being a part of the Departmental Offices domain). Since then, bureaus and offices have been divided (e.g., the Minerals Management Service), or have changed names (e.g., the Bureau of Trust Funds Administration), but the Department's AD still uses the old names. The "Background" section includes additional information on this breakdown.

Test 3: Formula-Specific Rules Plus Wordlist Attacks

Our next test was a formula-specific rules plus wordlist attack specifically designed to test for passphrases created by a popular online password generating tool.[37] This tool generates passphrases following multiple specific formulas intended to meet different complexity requirements typically used across different services or account types. It uses two or more dictionary words and inserts digits and special characters between and around them. We downloaded the site's dictionary and created rules to mimic the tool's "WEB16" and "NTLM" password format generation. We then created rules with three-word combinations similar to the site's "DEFAULT" password format generation, but found the tests were too complex to finish within a reasonable amount of time. We limited the types of special characters and combinations for this test to reduce the amount of time needed to complete the tests.

Test 4: Updated Wordlist

Finally, we generated a new wordlist using the passwords cracked during this inspection and performed Test 1 again.

[37] https://xkpasswd.net/s/.

Appendix 2: Response to Draft Report

The U.S. Department of the Interior's response to our draft report follows on page 33.

In addition to responding to our recommendations, Office of the Chief Information Officer (OCIO) provided two general comments and various technical comments. We updated our final report to address the Department's concerns where evidence and testimony supported its response. These updates did not change our findings or recommendations based on the evidence and controls as tested. We've summarized the OCIO's two general comments and responded to them below:

> **OCIO Comment 1:** The OCIO spent considerable time factually distinguishing the agency's situation from that of the Colonial Pipeline example cited in the report. More specifically, the OCIO stated that the "Department of the Interior's Risk Posture is very different from the referenced risks associated with the Colonial Pipeline Ransomware incident."
>
> **OIG Response:** The Colonial Pipeline ransomware attack is an example of the potential consequences of lack of multifactor authentication and weak account management practices. Although we acknowledge that the OCIO has identified what it believes to be various potential distinctions between the Colonial Pipeline situation and that of the Department (e.g., a different type of virtual private network), we did not verify these distinctions, as we did not attempt to compromise the Department's network by exploiting the vulnerabilities we found because such testing was out of scope. More fundamentally, although a breach to the Department's computer network could have a significant adverse effect on its operations, such a breach would not produce the same widespread disruption to businesses and consumers that resulted from the Colonial Pipeline IT security incident. We updated our report to include this information.
>
> **OCIO Comment 2:** "The significant difference between what the report suggests as the Department's status on Multi-Factor Authentication (MFA), versus the status of what has been implemented in the Department."
>
> **OIG Response:** Our report represents a snapshot in time and the conditions present during our fieldwork. The specific conditions related to password security existed when the OCIO extracted the hashes in February 2021. We provided our technical findings to the OCIO immediately as we discovered them to allow the OCIO to address the issues as quickly as possible. We did not review any additional guidance, progress, or new policy after our fieldwork ended in November 2021. We also provided the results of our analysis of the MFA status of all High Value Assets and informed the OCIO in November 2021 of our intent to report these numbers; we did not receive feedback from the OCIO at that time suggesting that these numbers were incorrect. We also note that, as the OCIO's responses to the various recommendations explain, the agency has not yet implemented steps needed to protect fully against the risks we have identified.

United States Department of the Interior

OFFICE OF THE SECRETARY
Washington, DC 20240

October 26, 2022

Memorandum

To: Mark Lee Greenblatt
Inspector General

Through: Darren B. Ash DARREN ASH Digitally signed by DARREN ASH Date: 2022 10 26 19:16:22 -04'00'
Chief Information Officer
Office of the Chief Information Officer

From: John Clink JOHN CLINK Digitally signed by JOHN CLINK Date: 2022.10.26 18:31:01 -04'00'
Acting Chief Information Security Officer
Office of the Chief Information Officer

Subject: Response to Draft Inspection Report - *P@s$w0rds at the U.S. Department of the Interior: Easily Cracked Passwords, Lack of Multifactor Authentication, and Other Failures Put Critical DOI Systems at Risk* (2021-ITA-005)

Thank you for providing the Department of the Interior (Department, DOI) the opportunity to review and comment on the draft Office of Inspector General (OIG) Report, *P@s$w0rds at the U.S. Department of the Interior: Easily Cracked Passwords, Lack of Multifactor Authentication, and Other Failures Put Critical DOI Systems at Risk (2021-ITA-005).*

We appreciate the effort and focus of this report and agree with the direction the OIG is proposing. We also would like to offer additional information that may clarify the report, primarily in the severity of risks identified and the inclusion of safeguards that protect the Department from potential exploitation. This report fundamentally asserts that passwords as lone credentials for authentication are not sufficient for modern information systems. The Department agrees and is committed to implementation of requirements specified in Executive Order (EO) 14028, *Improving the Nation's Cybersecurity* and related policies and directives.

If you have questions, please contact John Clink, Acting Chief Information Security Officer, at [redacted]@ios.doi.gov.

Attachment 1: General Comments

Attachment 2: Recommendations and Responses

cc: Deputy Chief Information Officers, OCIO
Naznin Rahman, Chief, Audit Management Division, Office of Financial Management
Bureau and Office Associate Chief Information Officers
Bureau and Office Associate Chief Information Security Officers
Bureau and Office Associate Chief Data Officers
Douglas Scoville, Chief, Governance Branch, OCIO
Richard Westmark, Chief, Compliance Management Section, OCIO

Attachment 1

General Comments to *P@s$w0rds at the U.S. Department of the Interior: Easily Cracked Passwords, Lack of Multifactor Authentication, and Other Failures Put Critical DOI Systems at Risk (2021-ITA-005)*

1. **Department of the Interior's Risk Posture is very different from the referenced risks associated with the Colonial Pipeline Ransomware incident**

This report draws some parallels between the Colonial Pipeline ransomware incident and the Department's current posture regarding multi-factor authentication (MFA) for users' access to sensitive systems and data. The Department appreciates the OIG's effort to bring attention to the potential risks of similar activity. Upon comparison, we found key distinctions that make the DOI risk level very different. The report points out that Colonial Pipeline was compromised due to stolen password credentials for an administrative account which was able to be used over Virtual Private Network (VPN). The compromised account had an old enough password in use that it was able to be found on the "dark web" and used by malicious actors to remotely access an enterprise network, where they used the credentials to further gain access to sensitive resources and install malware on them. The Department has key safeguards that lower the risk of exploitation from similar methods because of a defense-in-depth posture which includes the following:

a. Administrative accounts require PIV-based MFA. In this report, the OIG cited DOI's administrator accounts as 99% compliant with this requirement. A recent check to validate current compliance indicated 100% of DOI administrator accounts require PIV authentication.

b. The Department uses an Enterprise VPN, the only VPN allowed by policy and monitoring efforts. This VPN capability requires PIV-based authentication in order to access the network remotely. The VPN access control also performs various other checks on client access, to further mitigate the risk of malicious remote access in this manner.

c. The Department, in concert with the Cybersecurity and Infrastructure Security Agency (CISA), monitors the "dark web" for compromised user credentials. While we find many compromised passwords, they are nearly always old credentials which have since been changed. Most often, the compromised passwords are not compliant with DOI Windows Domain password requirements, and therefore, are not indicative of a password that was ever used for network access.

d. The Department monitors server privileged access, malicious attempts to change server configuration or install malware. While no monitoring is perfect, DOI monitoring success has improved sensitive system and data protection. Analysis of the current technical realities show that DOI's risk posture is far lower than what was characterized in the report for Colonial Pipeline. We believe that DOI should prioritize implementing OMB requirements and corrective actions.

2. **The significant difference between what the report suggests as the Department's status on Multi-Factor Authentication (MFA), versus the status of what has been implemented in the Department.**

The Department agrees with the OIG assertion that the applications which are serving users and providing access to sensitive data and services need to be protected by MFA. The Department has been working for several years with direction from the Office of Management and Budget (OMB) to make this transition. Recently, OMB released M-22-09, *Moving the U.S Government Toward Zero Trust Cybersecurity Principles* (January 2022), which provides requirements for this transition. The Department is in compliance with M-22-09.

The Office of the Chief Information Officer (OCIO) released OCIO Memorandum, *Implementation of Multi-Factor Authentication using Phishing-Resistant Credentials Directi*ve, dated August 26, 2022 requiring application owners to make this transition within the time frame required by OMB. The OIG is correct in asserting single-factor, password-based authentication is problematic and higher risk. The Department is responsive to OMB guidance to move away from password-based authentication entirely and has begun this activity in partnership with CISA, the Department of Homeland Security (DHS), and OMB. The Department has been responsive to OMB's requirements with regard to multi-factor authentication guidance, policy, requirements, and law. A vast majority of all authentications occurring on DOI systems are multi-factor based. The analysis cited for DOI High Value Assets (HVAs) seems to be based on a misunderstanding of the Department's answers to OMB's Federal Information Security Modernization Act (FISMA) Metrics regarding MFA compliance. Prior to FY 2022, OMB's FISMA Metrics asked for counts of HVAs using MFA for 100% of user authentications. This meant that an HVA using MFA to protect access to sensitive data and processes but allowing password access to a non-sensitive component of the system had to be excluded from the count of HVAs using MFA. OMB recognizes the complexity of moving to MFA and set a target date of 2024 to complete this transition. The Department has required PIV authentication for Windows Domain Server administration accounts and access to the VPN. The Department has exceptions in place-based technologies in use while we are currently in the middle of a transition based on M-22-09 requirements, which will allow user access to any resource to be restricted to PIV or other MFA alternative access only. The Department agrees with and appreciates the OIG's position that this should occur and is making efficient progress to achieve this OMB requirement.

Attachment 2

Management Responses to *P@s$w0rds at the U.S. Department of the Interior: Easily Cracked Passwords, Lack of Multifactor Authentication [MFA], and Other Failures Put Critical DOI Systems at Risk (2021-ITA-005)*

Recommendations and Responses

All recommendations are issued to the Department of the Interior.

Recommendation 1: Prioritize implementing PIV or other Department-approved MFA methods that cannot be bypassed to allow single-factor authentication for all applications, starting with the Department's HVAs.

Response: Concur. The Department is currently working to meet the MFA implementation requirements of Executive Order (EO) 14028, *Improving the Nation's Cybersecurity* (May 2021) and Office of Management and Budget (OMB) M-22-09, *Moving the U.S Government Toward Zero Trust Cybersecurity Principles* (January 2022), which are government-wide efforts to migrate the Federal Government to a Zero Trust Architecture. Our progress includes the issuance of the Zero Trust Strategy and OCIO Memorandum, *Implementation of Multi-Factor Authentication using Phishing-Resistant Credentials Directi*ve, dated August 26, 2022, which directs all bureaus and offices to enforce MFA through the Department's approved phishing-resistant MFA services for all information systems and establishes prioritization of Department-approved MFA methods across the agency. The Department and the bureaus and offices will take a risk-based approach in prioritizing the conversion of systems and applications from legacy authentication methods to MFA.

Responsible Official: John Clink, Acting Chief Information Security Officer

Target Date: December 30, 2024

Recommendation 2: Develop and implement a process to track and validate MFA status for all Department information systems.

Response: Concur. On August 26, 2022, the DOI OCIO issued a memorandum with subject, *Implementation of Multi-Factor Authentication using Phishing-Resistant Credentials Directi*ve, requiring all bureaus and offices to enforce MFA through the Department's approved phishing-resistant MFA services for all information systems no later than the end of FY 2025. The DOI OCIO will develop a process to track compliance with this memorandum.

Responsible Official: John Clink, Acting Chief Information Security Officer

Target Date: April 30, 2023

Recommendation 3: Revise password complexity and account management policies to reflect the updated risk-based approach set forth in the NIST SP 800-63 document suite, such as using longer passphrases and less frequent change intervals.

Response: Concur. The Department is in the process of revising its Security and Privacy Control Standards to adopt the recommendations of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63 as specified in M-22-09. The new Departmental password complexity and account management policies will take effect upon issuance of the revised Security and Privacy Control Standards. Bureaus and offices will then be afforded a reasonable period to implement the new policies.

Responsible Official: John Clink, Acting Chief Information Security Officer

Target Date: January 26, 2023

Recommendation 4: Implement controls to monitor, limit, or prevent commonly used, expected, or compromised passphrases and passwords in accordance with NIST SP 800–63 and NIST SP 800–53.

Response: Concur. Regarding Active Directory (AD) accounts managed by OCIO, the Department will implement Azure AD Password Protection.

Responsible Official: John Clink, Acting Chief Information Security Officer

Target Date: March 31, 2024

Recommendation 5: Prioritize the inventory, monitoring, and enforcement of existing controls as well as the controls we recommended in this report for accounts belonging to senior Government employees or accounts with elevated privileges.

Response: Concur. The Department already prioritizes the monitoring and enforcement of controls for accounts handling sensitive information and/or privilege access. This provides leadership appropriate authority and flexibility to manage risk. For the tested domain, DOI.Net, domain administrative accounts are very restrictive and monitored closely. Server administrators are less restrictive; therefore, the Department has inventory and monitoring for their identity activity.

Responsible Official: John Clink, Acting Chief Information Security Officer

Target Date: Not Applicable

Recommendation 6: Revise account management policy to prohibit related accounts from using the same passphrases and passwords (e.g., shared mailboxes, service accounts, or users with multiple service-level accounts).

Response: Concur. The Department will revise authenticator management policy to manage risk posed by re-use of passwords across multiple system accounts.

Responsible Official: John Clink, Acting Chief Information Security Officer

Target Date: January 26, 2024

Recommendation 7: Implement guidance requiring temporary passphrases and passwords to be unique and complex, rather than using a common variation or reusing the same passphrase or password.

Response: Concur. The Department has drafted new password complexity and length policies to comply with M-22-09. The OCIO will review this draft policy in light of this recommendation and ensure that our policies meet M-22-09.

Responsible Official: John Clink, Acting Chief Information Security Officer

Target Date: May 1, 2023

Recommendation 8: Establish procedures and accountability mechanisms to ensure compliance with policies regarding account management monitoring and timely disabling of inactive accounts.

Response: Concur. The OCIO has existing procedures and mechanisms to implement policies regarding disabling of inactive accounts. User (people) AD accounts are automatically disabled when the accounts are flagged in the DOIAccess system as no longer needing DOI access. The accounts must be flagged in DOIAccess by Human Resources (for Federal employees) or Contracting Officers or their Representative. The OCIO and other relevant program offices will work with bureaus and offices to ensure that practices are consistently implemented to ensure accounts that need to be disabled are flagged in a timely manner. Contractor account management controls will be strengthened to improve status monitoring for timely disabling.

Responsible Official: John Clink, Acting Chief Information Security Officer

Target Date: January 26, 2024

Appendix 3: Status of Recommendations

Recommendation	Status	Action Required
1–3, 7	Resolved but not implemented	We will refer these recommendations to the Office of Policy, Management and Budget (PMB) to track implementation.
4, 6, 8	Resolved but not implemented	The U.S. Department of the Interior should revise its target implementation dates for these recommendations and provide the revised dates to the PMB. We will refer these recommendations to the PMB to track implementation.
5	Unresolved	We will refer this recommendation to the PMB for resolution.

OFFICE OF
INSPECTOR GENERAL
U.S. DEPARTMENT OF THE INTERIOR

REPORT FRAUD, WASTE, ABUSE, AND MISMANAGEMENT

The Office of Inspector General (OIG) provides independent oversight and promotes integrity and accountability in the programs and operations of the U.S. Department of the Interior (DOI). One way we achieve this mission is by working with the people who contact us through our hotline.

☎ If you wish to file a complaint about potential fraud, waste, abuse, or mismanagement in the DOI, please visit the OIG's online hotline at **www.doioig.gov/hotline** or call the OIG hotline's toll-free number: **1-800-424-5081**

Who Can Report?

Anyone with knowledge of potential fraud, waste, abuse, misconduct, or mismanagement involving the DOI should contact the OIG hotline. This includes knowledge of potential misuse involving DOI grants and contracts.

How Does it Help?

Every day, DOI employees and non-employees alike contact the OIG, and the information they share can lead to reviews and investigations that result in accountability and positive change for the DOI, its employees, and the public.

Who Is Protected?

Anyone may request confidentiality. The Privacy Act, the Inspector General Act, and other applicable laws protect complainants. Section 7(b) of the Inspector General Act of 1978 states that the Inspector General shall not disclose the identity of a DOI employee who reports an allegation or provides information without the employee's consent, unless the Inspector General determines that disclosure is unavoidable during the course of the investigation. By law, Federal employees may not take or threaten to take a personnel action because of whistleblowing or the exercise of a lawful appeal, complaint, or grievance right. Non-DOI employees who report allegations may also specifically request confidentiality.