STATEMENT
OF
THE HONORABLE MARK LEE GREENBLATT
INSPECTOR GENERAL
U.S. DEPARTMENT OF THE INTERIOR

BEFORE THE
HOUSE COMMITTEE ON NATURAL RESOURCES
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

"EXAMINING ONGOING CYBERSECURITY THREATS WITHIN THE DEPARTMENT OF THE INTERIOR AND THE NEXUS TO STATE-SPONSORED CYBER ACTORS"

JUNE 7, 2023

Chairman Gosar, Ranking Member Stansbury, and Members of the Subcommittee, thank you for giving me the opportunity to discuss cybersecurity at the Department of the Interior (DOI) and in particular, our office's January 2023 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*. As you know, inspectors general have a direct reporting relationship to Congress. My office and I take this obligation seriously, and we appreciate the Subcommittee's continued support for our independent and objective oversight.

In our recent inspection of the DOI's password security, we found that the DOI's management practices and password complexity requirements were not sufficient to prevent potential unauthorized access to its systems and data. In fact, during 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. As the result of our findings, we made eight recommendations to help the Department strengthen its IT security by improving user account management practices. The DOI concurred with our recommendations.

I. Background

The DOI Office of Inspector General (OIG) has recognized IT security as one of the DOI's top management challenges for many years. The DOI relies on complex, interconnected information systems to carry out its daily operations and spends approximately $1.7 billion annually on its portfolio of IT assets. Our work has found that the DOI continues to face challenges in implementing an enterprise IT security program that balances compliance, cost, and risk while enabling bureaus to meet their diverse missions.

The OIG prioritizes cybersecurity oversight as an important part of our portfolio. For example, our 2023-2024 oversight plan includes planned reviews of the DOI's vulnerability remediation practices and cyber threat hunting efforts. We also currently have an ongoing review of the DOI's public cloud computing security practices.

In April 2023, we issued the fiscal year 2022 annual independent Federal Information Security Modernization Act (FISMA) audit for the DOI.[1] That audit identified needed improvements and made 24 recommendations intended to strengthen the DOI's information security program as well as those of the bureaus and offices. Using FISMA metrics, the Office of Management and Budget (OMB) scored the cybersecurity performance of 23 Federal agencies, including the DOI. The DOI scored a 68 percent and ranked 23rd on the list.

Other recent work published by our office includes the results of our testing of the DOI's cyber threat detection and defense controls. Specifically, in August 2022, we issued a memorandum concluding that this evaluation could be closed without a full-scale report because we were satisfied with the Department's response to our technical tests, conducted between May and November 2021.[2] Our review of the Department's cyber incident tracking system demonstrated that the DOI's IT staff identified our simulated attacks. Moreover, the Department mitigated confirmed technical vulnerabilities identified by our technical tests.

In addition, in September 2020, we issued a report of our evaluation of the security of the DOI's wireless networks.[3] Our evaluation revealed that the Department did not deploy and operate a secure wireless network infrastructure. We conducted reconnaissance and penetration testing of wireless networks representing each bureau and office. To do this, we assembled portable test units for less than $200 that were easily concealed in a backpack or purse and operated these units with smartphones from publicly accessible areas and locations open to visitors. Our attacks simulated the techniques of malicious actors attempting to break into departmental wireless networks, such as eavesdropping, so-called "evil twin" attacks,[4] and password cracking. We made 14 recommendations that will help prevent malicious actors from eavesdropping on internal communications and gaining unauthorized access to the DOI's wireless networks. The Department concurred with and has implemented all recommendations.

Given the team's success rate cracking passwords during our September 2020 evaluation, we decided to conduct a formal test of passwords throughout the Department. That prompted this passwords project, in which we inspected the DOI's password complexity requirements after defining rules of engagement[5] with the Department to ensure that it was able to protect its IT systems and that any vulnerabilities could be addressed promptly.

---

[1] *Summary: Independent Auditors' Performance Audit Report on the U.S. Department of the Interior Federal Information Security Modernization Act for Fiscal Year 2022* (Report No. 2022–ITA–028).

[2] *The U.S. Department of the Interior's Cyber Threat Detection and Defense Controls* (Report No. 2020–ITA–067).

[3] *Evil Twins, Eavesdropping, and Password Cracking: How the Office of Inspector General Successfully Attacked the U.S. Department of the Interior's Wireless Networks* (Report No. 2018–ITA–020).

[4] In such attacks, bad actors seek to capture usernames and passwords and then crack the passwords.

[5] As explained in our report, 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.

II. The DOI OIG's Inspection of the DOI's Password Complexity Requirements

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. In this inspection, 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.

A. Methodology

A "clear text password" is what a user types when prompted to log in to a system. To avoid exposing a sensitive password, user passwords are stored in a secure, unintelligible format called "hashes." 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. So, for example, the clear text password "Password-1234" is stored in its hashed form as "A71FB31235347EA75956B6155ED36899."

Hashes are generally considered secure because they cannot be directly reverted to clear text—their original state. However, there are indirect methods attackers can use to attempt to recover hashed passwords. Once attackers have captured hashes, they must attempt to recover their original clear text form through a process referred to as "hash cracking."[6] If successful, this enables the attacker to use the password to gain unauthorized access to an organization's computer systems and data.

To test the Department's passwords, our inspectors spent less than $15,000 on a system designed to crack—or hack—passwords using open-source software and a custom wordlist, consisting of publicly available password lists harvested from past data breaches, dictionaries from multiple languages, U.S. Government terminology, and pop culture references. We created a set of rules and processes for manipulating and combining those words into password candidates; we then attempted to crack the hashes for every DOI user account.[7]

B. Findings

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,

[6] "Hash cracking" is the automated process of generating clear text password "candidates" 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.

[7] 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.

including 288 accounts with elevated privileges and 362 accounts of senior U.S. Government employees.

Specifically, we found that:

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

2. 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.

3. 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 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"; at the time of our report, this combination met the Department's requirements, even though it is not difficult to crack.

4. 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.

The Department Did Not Consistently Implement MFA on Its Systems

MFA refers to the requirement to use at least two factors to access computer systems, such as a password plus a PIN from a smartphone app or a PIV card plus a password. When MFA is implemented correctly, it adds a layer of security that protects organizations, even when passwords are compromised.

MFA is already required on all Federal information systems and has been for decades. As our inspection showed, however, the Department still allowed single-factor authentication (username and password) on an indeterminate number of its systems, including high-value IT assets.

Because the Department relied on authentication methods that were not in line with National Institute of Science and Technology (NIST) recommendations, Governmentwide mandates, and industry best practices, the burden of the Department's security controls rested on obsolete password complexity requirements. Further, the Department did not have a full picture of which systems complied with which standards. Without requiring and enforcing MFA across its systems—including those that contain sensitive information—the Department's data remains at risk of unauthorized exposure.

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

Department policy at the time of our inspection required 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. 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.

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—all of which people tend to use to construct memorable passwords. Although the Department's password policy at the time of the inspection appeared to encourage complex passwords, in practice, its policies were not sufficient to prevent users from creating passwords that are easy to crack.[8]

Further, 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 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. This creates a feedback loop that frustrates users, perpetuates the weak password cycle, and does not improve security.

The Department's Password Complexity Requirements Implicitly Allowed Hundreds of Unrelated Accounts To Use 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. We found that the same easy-to-crack passwords (which all met the Department's complexity requirements) were used across multiple active accounts. 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.[9]

[8] 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 complexity requirement. 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 letters, lowercase letters, digits, and a special character, it is, in fact, easy to crack.

[9] In other cases, we found common passwords reused across multiple related accounts, such as new accounts with temporary passwords, shared mailboxes, or service accounts. (Service accounts are often granted elevated privileges over systems or data, and shared mailboxes often contain sensitive data or attachments.) Understanding 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.

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.

NIST standards require 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 Department's bureaus had implemented the ability to check for and prevent weak passwords.

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 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, as they offer more opportunities for a malicious actor to gain unauthorized access. Disabling accounts after a period of inactivity reduces this risk. We found that 6,243 of all active accounts had not been used for more than 45 days; the Department failed to disable these accounts as required by 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.

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. Without that password age limit, an attacker is not limited by time. According to Department policy in place at the time of our inspection, an attacker would have only 60 days to intercept or otherwise acquire a hash, crack it, and then use it.

C. Recommendations

Given our findings, we made eight recommendations to the Department to help it strengthen its IT security by improving account management practices. In summary, our recommendations can be grouped into four broad categories:

- First, we recommended that the Department prioritize implementing MFA across all systems and develop a system to track the status of the implementation of MFA.
- Second, we recommended that the Department revise password complexity requirements to bring them in line with current NIST guidance, such as using longer passphrases and less frequent change intervals.
- Third, we recommended that the Department revise policy to prohibit accounts from reusing the same passphrases and passwords.
- Fourth, we recommended that the Department ensure compliance with policies regarding timely disabling of inactive accounts.

In response to the report, the Department concurred with our recommendations and provided target implementation dates. We are engaged in ongoing communication with the Department regarding the status of these recommendations and will report on Oversight.gov when actions sufficient to close the recommendations have occurred.

III. 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.

The Department's reliance on single-factor authentication only increased the importance of aligning its account management requirements with NIST's recommendations.

To best mitigate the risk of easy-to-crack passwords, the Department should prioritize MFA on all systems and applications. In those instances where MFA has not yet been implemented, password complexity requirements should be updated to comply with NIST guidance.

Thank you for your time. I look forward to answering questions.