EVALUATION

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

U.S. Bureau of Reclamation Selected Hydropower Dams at Increased Risk From Insider Threats

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

Report No.: 2017-ITA-023

June 2018

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

Memorandum

JUN 07 2018

To: Brenda Burman
Commissioner, U.S. Bureau of Reclamation

From: Mary L. Kendall Mary L Kendall
Deputy Inspector General

Subject: Final Evaluation Report – U.S. Bureau of Reclamation Selected Hydropower Dams at Increased Risk from Insider Threats
Report No.: 2017-ITA-023

This memorandum transmits the findings of our evaluation of the U.S. Bureau of Reclamation's (USBR's) technical and managerial practices for protecting its hydropower producing dams, categorized as critical infrastructure, from emerging cyber threats. The USBR operates five hydropower dams categorized as critical infrastructure. For two of these dams, the USBR relies on an industrial control computer system to remotely control operations including, generators, gates, and outlet valves. We make five recommendations to help the USBR improve the security posture of its critical dams by mitigating insider threats to its industrial control system.

In response to our draft report, the USBR partially concurred with two recommendations and did not concur with three recommendations. Based on this response, we consider all five recommendations unresolved. We will forward them to the Office of Policy, Management and Budget for resolution and to track their implementation.

If you have any questions regarding this report, please contact me at 202-208-5745.

The legislation creating the Office of Inspector General requires that we report to Congress semiannually on all audit, inspection, and evaluation reports issued; actions taken to implement our recommendations; and recommendations that have not been implemented.

Table of Contents

Results in Brief

We assessed U.S. Bureau of Reclamation's (USBR's) operational and technical practices for protecting two of its hydropower dams categorized by the U.S. Department of Homeland Security as critical infrastructure from emerging cyber threats.[1] The USBR operates five hydropower dams categorized as critical infrastructure. For two of these dams, the USBR relies on an industrial control computer system to remotely control operations including, generators, gates, and outlet valves.

We found the industrial control system (ICS) at low risk of compromise from external cyber threats as our analysis of computer network traffic showed that ICS is isolated from the internet and from USBR's business systems and our analysis of the ICS computer memory did not detect hidden malware or other indicators of compromise. USBR's account management and personnel security practices, however, put the ICS and the infrastructure it operates at high risk from insider threats. Specifically, we found that the USBR:

- Failed to limit the number of ICS users with system administrator access and had an extensive number of group accounts

- Did not comply with password policies and failed to remove inactive system administrator accounts

- Did not follow best practices recommending that personnel with elevated system privileges complete more rigorous background investigations

These deficiencies occurred because USBR management failed to strengthen bureau risk management practices in response to rapidly escalating threats to critical infrastructure. An ICS breach could disrupt USBR operations and has the potential to adversely affect national security. We make five recommendations to help the USBR improve the security posture of its critical dams by mitigating insider threats to its ICS.

[1] According to the U.S. Department of Homeland Security, "critical infrastructure" are those systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

Introduction

Objective

We assessed the U.S. Bureau of Reclamation's (USBR's) operational and technical practices for protecting two of its hydropower dams categorized as critical infrastructure from emerging cyber threats. Specifically, we analyzed terabytes of computer network traffic and computer memory for the systems used to operate and support USBR's dams for hidden malware and other indicators of compromise. We also evaluated USBR's practices for managing and monitoring users with Super User (i.e., system administrator) privileges to the industrial control system (ICS).

This evaluation is the first in a series assessing the cyber security of USBR hydropower dams categorized as critical infrastructure. Appendix 1 provides further details regarding our scope and methodology.

Background

The U.S. Department of Interior spends about $1.2 billion annually on its information technology (IT) asset portfolio, which includes computer systems that support bureau programs which, protect and manage our Nation's natural resources, provide scientific information to stakeholders, and help meet obligations to Native American communities.

The Department's IT asset portfolio also includes ICS used by USBR to support the generation and transmission of hydroelectric power. Unlike traditional IT systems where computers store and process data to support administrative functions such as Finance and Human Resources; ICS use computers to control electrical, mechanical, hydraulic, or pneumatic components to achieve a physical outcome. For example, industrial control systems operate circuits that transmit electricity from a dam to a substation and open and close valves to control flow in an oil pipeline. Industrial control systems play a key role in the operation of the Nation's critical infrastructure including power plants and dams as well as energy production, distribution, and transportation systems.

Since 2009, the U.S. Department of Homeland Security (DHS) has issued alerts and advisories about suspicious cyber activity, incidents, and vulnerabilities affecting critical infrastructure monitored and controlled by ICS. Specifically, ICS are increasingly vulnerable to targeted malware which enables an attacker to cause an infected ICS to malfunction. For example, the attacker may prevent valves on an oil pipeline from opening or closing as needed or cause turbines in a hydropower generator to spin at dangerously high speeds. DHS's Industrial Control Systems Cyber Emergency Response Team reported 290 cyber-attacks on critical infrastructure control systems in fiscal year 2016.

USBR, the Nation’s second largest producer of hydroelectric power, uses ICS to support the generation and transmission of hydroelectric power. Annually, USBR hydroelectric plants generate over 40 billion kilowatt hours of electricity meeting the residential needs of over 3.5 million homes.[2] The electricity is primarily produced at 53 hydroelectric power plants operated by USBR.[3]

Historically, ICS were physically isolated from an organization’s traditional IT systems, as well as from the internet, and thus could be protected from unauthorized access using physical security measures (e.g., guards, fences, and locks). Over time, to promote connectivity, efficiency, and remote access capabilities, ICS have become interconnected with an organization’s traditional IT systems, rendering physical measures inadequate to secure these networks.

In recent years, nation-states such as Russia have targeted critical infrastructure including electric power generators and distributors by infecting industrial control systems that operate the infrastructure with sophisticated malware. For example, ICS operated by Ukrainian electric power distribution companies were infected with sophisticated malware. Once infected, the remote attackers caused Ukraine power companies’ industrial control systems to malfunction, which resulted in power outages affecting hundreds of thousands of customers. Malware analysis performed by DHS in conjunction with U.S. private sector IT security firms determined that the affected entities were breached about nine months prior to the outages.

These types of attacks are able to occur because the ICS network was not isolated from the business systems and internet. As such, remote attackers can put malware on the ICS by sending emails with malicious payloads to employees that operated the industrial control systems. When the employee accessed the email and downloaded a file or clicked a link in the email, the employee’s computer was infected giving the remote attacker a foothold on the organization’s computer network. These cyber threats bypassed firewalls and went undetected by the organization’s intrusion detection system and antivirus software. Moreover, the use of group accounts (accounts shared by multiple individual users) on these systems make it harder to detect inappropriate logons and activity ultimately delaying response to the incidents

Combating cyber threats to critical infrastructure requires acknowledging that traditional cyber defenses—firewalls, intrusion detection systems, and antivirus software often fail to deter or detect sophisticated malware. As a best practice, organizations may assume the systems that operate infrastructure are already potentially compromised, and search the computer networks that operate infrastructure for hidden malware. This proactive approach is referred to as “threat hunting,” which includes, but is not limited to, capturing and analyzing

[2] USBR Website: https://www.usbr.gov/power/who/who.html
[3] USBR Website: https://www.usbr.gov/power/who/who.html

computer network traffic for malicious communications and dissecting computer memory to find malware.

While isolating ICS from business systems and the internet may deter external cyber threats, insider threats from employees, contractors, and service providers who have legitimate access to ICS still exist. Insiders, particularly those with system administrator access, can use their intimate knowledge of the ICS in combination with their elevated system privileges to bypass controls and potentially disrupt mission operations. Further, because insiders are authorized to use the systems, these individuals may not be detected immediately when they access ICS for unauthorized purposes. Accordingly, the greatest insider threat risk is from individuals who have system administrator access privileges to the ICS. These users can essentially perform all functions within the systems (e.g., uploading software, downloading sensitive files and modifying data, adding and removing users, changing hardware and software configurations, and altering audit logs to conceal their actions).

Findings

While our threat hunting[4] activities did not detect malware or other indicators of compromise on the ICS and business systems used to operate and support USBR's dams, we found significant control weaknesses in USBR's account management and personnel security practices, leaving hydropower operations at the dams at an increased risk from insider threats. Specifically, we found that the USBR:

- Did not limit the number of ICS users with system administrator access and had an extensive number of group accounts
- Did not comply with password policies and failed to remove inactive accounts
- Did not require personnel with elevated system privileges to complete more rigorous background investigations

These deficiencies occurred because USBR management failed to strengthen bureau risk management practices in response to rapidly escalating threats to critical infrastructure. A breach of the ICS could have a serious adverse effect on bureau operations, assets, and individuals.

Based on our forensic analysis of ICS network traffic and computer memory, we concluded that risk of ICS compromise from external cyber threats is low because:

- The ICS is isolated from USBR's general support system and from the internet.
- Inbound connections to the ICS network are not allowed from external networks.
- Outbound connections are restricted to other ICS computers operating USBR dams.
- The USBR implemented controls to prevent malware infections from external media such as thumb drives.
- The USBR has a complete IT asset inventory for the ICS.

[4] Threat hunting involves actively searching information technology systems for hidden malware and indicators of compromise under the assumption that attackers may have already compromised the systems because traditional cyber defenses cannot prevent all attacks.

- Malware or other indicators of compromise were not identified.

Critical Hydropower Dams at Increased Risk of Insider Threats

Our evaluation of USBR's account management and personnel security practices identified significant control weaknesses that could be exploited by insiders. The USBR failed to limit the number of ICS users with system administrator access. More troubling, USBR authorized 18 ICS group accounts with system administrator access, even though tracing ICS changes back to the one who made the change is impossible and thus a significant control deficiency.

The USBR also did not require personnel with elevated system privileges to complete more rigorous background investigations, a widely recognized best practice used to reduce risk.

Excessive Number of Employees with System Administrator Access

The U.S. Secret Service and the Carnegie Mellon Software Engineering Institute's Insider Threat Study[5] analyzed acts of insider sabotage on computer systems in critical infrastructure sectors and found that the majority of insiders who committed the attacks were granted system administrator access and had access to group accounts. As part of mitigating risks related to users with elevated system privileges, the National Institute for Standards and Technology (NIST) states that organizations should implement "least privilege" by limiting the number of employees with system administrator access to a small subset of users based on their official duties. Limiting system administrator access to a small subset of users and continuously monitoring activities associated with these accounts can help mitigate the risk of insider threats. Section 1(c)(ii) of the May 11, 2017 Executive Order on *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* emphasizes the importance of following NIST recommendations for cybersecurity because it requires that executive agencies, including the Department of the Interior, follow NIST criteria to mitigate cybersecurity risks.

We found that the ICS did not implement the principle of "least privilege" by limiting the number of employees with system administrator access based on employees' defined workplace roles and responsibilities, as the NIST required. During our April 2017 visit, we found that the USBR Operations Center had 25 employees, 24 of them with active individual ICS accounts. Thirteen of the 25 employees (52 percent) also had access to at least one other ICS account with system administrator access. Our review of USBR position designations for the 13 employees, however, showed that only 5 had ICS administration related duties defined in their position designations. By not limiting the number of users with

[5] The United States Secret Service and the Carnegie Mellon Software Engineering Institute, Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors, May 2005

system administrative access, the USBR has increased the risk of ICS loss or disruption from an employee mistake or the deliberate act of a malicious insider.

Extensive Use of Group Accounts with Administrator Access

The NIST also requires agencies to establish conditions and roles for group user accounts. Group accounts (accounts where a single logon credential, such as a password is shared among two or more individuals) should be minimized. The use of group accounts does not provide for individual accountability because system changes cannot be traced back to a specific user. For this reason, best practices dictate that group accounts having system administrator access should be limited. Also, an integrity mechanism to detect any modification of security and user logs should be implemented. *NIST 800-53 Rev. 4 control AC-2* establishes requirements for creating, modifying, disabling, and removing accounts; monitoring the use of accounts; reviewing accounts for compliance; and establishing a process for reissuing shared account credentials when individuals are removed.

We found that the USBR authorized 18 ICS group accounts with system administrator access. Each of the 18 accounts were shared among 11 employees. A large number of shared accounts increases the likelihood that unauthorized individuals may access account due to inadvertent disclosure.

In addition to not following “least privilege” principle, USBR’s extensive use of group accounts did not fulfill the NIST requirement that all system actions performed from accounts having elevated privilege be continuously monitored, ensuring that an audit trail leads back to the employee making the change. For the 18 ICS group accounts, passwords are shared among 11 people, making it impossible to enforce an individual’s accountability for ICS changes made while using group accounts.

The USBR justified the large number of system administrator and shared accounts because a user account must remain logged on to allow ICS applications and services to function properly. The USBR also stated that because ICS provides 24/7 support to Bureau hydropower dams, at least 12 bureau staff with system administrator access are needed to cover the three 8-hour shifts.

We contacted the U.S. Army Corps of Engineers, the Nation’s largest producer of hydroelectric power, to discuss its approach to group accounts with elevated privileges. We inquired about Federal employees implementing computer security programs for the hydroelectric power dams. The Corps prohibits the use of such accounts for the security reasons already stated.

Overall, the USBR’s excessive number of employees and group accounts with elevated privileges significantly increase the risk that the ICS may experience loss or disruption, whether caused deliberately or by accident. With system administrator access, a malicious insider could:

- Install malware and cause the ICS to malfunction, potentially disrupting dam operations

- Install a “back door” to enable unmonitored access to the ICS

- Delete or modify critical system configuration files and programs

- Revoke user privileges, preventing authorized users from accessing the system

- Delete or modify system logs to conceal malicious actions or shift blame to another ICS user

Finally, if system administrator privileges are loosely and widely distributed, as with USBR’s ICS, potential attackers have a much easier time gaining full control of the system. Under these circumstances, multiple accounts with elevated privileges can act as avenues through which an attacker can compromise the system.

Non-Compliance with Password Policies and Failure to Remove Inactive Accounts

According to the NIST, employee termination procedures should include disabling access to all accounts to which that user had access, including shared accounts. Department policy requires that inactive accounts be disabled after 90 days and that passwords be changed every 60 days. The use of shared accounts makes it difficult to coordinate and communicate password changes to all shared account holders, however, thus promoting poor IT security practices. Not changing group passwords for shared accounts, including system administrator accounts, when an employee leaves exposes the organization to a vulnerability easily exploited by a former employee possessing the shared password.

We found that the USBR did not implement controls to facilitate continuously reviewing user accounts to ensure inactive accounts are removed and ensure that passwords are continuously updated. Specifically, we found that:

- Nine of the 30 ICS administrator accounts have not been used for at least a year.

- Ten of the 30 administrator accounts have not had the password changed for at least a year.

- Seven of the 18 shared administrator (group) accounts have not been used for at least a year.

These deficiencies occurred because the USBR failed to monitor accounts to ensure that inactive accounts were removed and passwords changed, thus increasing the risk that these accounts could be used for malicious purposes. USBR's ICS is a moderate-impact system. The breach of such a system can have a serious adverse effect on USBR operations, assets, and individuals.

Weak Personnel Security Practices for USBR Employees Administering the ICS

An industry best practice to help mitigate insider threat risks includes establishing risk management practices that put additional scrutiny on individuals who administer an organization's most important IT assets, including its ICS. Specifically, background investigations should be tailored to an individual's threat risk, based on his or her official duties. For example, the National Security Agency recommends that personnel with elevated system privileges (i.e., system administrators) undergo more rigorous background investigations to reduce risk.

We found that the USBR did not follow National Security Agency best practices. As part of our evaluation, we obtained background investigation and position designation information for the 13 USBR employees with system administrator access to the ICS. We found that 11 of 13 had completed a Tier 2 background investigation for a position designated as a moderate risk public trust position. We also reviewed the USBR's personnel security policy, which prescribes the level of background investigation (Tier 1 up to Tier 5), and whether a position is designated as a public trust or a national security position. The USBR's personnel security manual indicates that IT positions with system administrator access to cyber assets supporting critical infrastructure (i.e., the ICS) undergo the same background investigation (Tier 2) as IT positions without system administrator access to cyber critical assets.

We also found that the USBR's personnel security practices lagged behind other Federal agencies' practices using ICS to operate hydropower dams. The Tennessee Valley Authority, the Nation's third largest producer of hydroelectric power, as well as the U.S. Army Corps of Engineers require those administering and securing the ICS to undergo at least a Tier 3 background investigation and maintain a Secret level security clearance.

In addition, we found that the ICS' privileged users did not receive continuous evaluation as required by the 2012 Federal Investigative Standards because USBR personnel did not have background investigations for the Secret level and above. The USBR's use of shared accounts also increased these risks because they could more easily allow a malicious insider to conceal malicious actions or shift blame to another user. Continuous evaluation of employees who have access to critical systems is required to evaluate any changes in employees' life circumstances that could increase insider threat risks.

This deficiency occurred, we believe, because the USBR did not re-evaluate the level of background checks it needed to protect its critical infrastructure, especially considering the increased cyber threat environment, particularly with the rapid escalation and sophistication of attacks targeting ICS that operate critical infrastructure.

Recommendations

We recommend that the USBR:

1. Implement "least privilege" by limiting the number of USBR employees with elevated privileges to its ICS based on the official duties listed in their respective position designations.

2. Eliminate all ICS group accounts with elevated privileges and prohibit the use of such accounts in all USBR systems that support Bureau hydroelectric power dams.

3. Implement controls to ensure that ICS user accounts are removed when no longer needed in accordance with DOI policy.

4. Implement controls to ensure that passwords are regularly changed for ICS user accounts in accordance with DOI policy.

5. Establish and implement procedures to ensure additional background scrutiny commensurate with a risk analysis of each employee's privileges to the ICS and industry best practices

Conclusion and Recommendations

Conclusion

Cyber attacks against industrial control systems that operate critical infrastructure are escalating. As such, the USBR must strengthen its security practices to minimize risk of disruption to its major hydropower producing dams. Until the USBR improves its risk management practices, its ICS and the critical infrastructure it operates will remain at increased risk of compromise, which could disrupt USBR mission operations and potentially affect national security.

Recommendation Summary

In response to our draft report, the USBR partially concurred with two recommendations and did not concur with three recommendations. We consider all five recommendations to be unresolved and we are referring them to the Assistant Secretary for Policy, Management and Budget for resolution. The USBR's full response is included in Appendix 2. Appendix 3 lists the status of each recommendation.

[redacted]

To reduce the risk of threats from insiders on critical infrastructure, we recommend that the USBR:

1. Implement "least privilege" by limiting the number of USBR employees with elevated privileges to [redacted] based on the official duties listed in their respective position designations.

   USBR Response: The USBR did not concur with Recommendation 1. The USBR stated that it has implemented least privilege in accordance with NIST guidance by only authorizing the elevated privileges necessary to accomplish assigned tasks in accordance with mission requirements. The USBR stated that elevated privileges are only granted to USBR employees who administer the system or network, provide technical support or perform cybersecurity-related functions. The USBR said that 13 of the 25 employees (52 percent) have elevated privilege accounts since the operations center is responsible for providing system operations and maintenance for the entire ICS system. That percentage is not representative for the entire system, since there are over 100 active accounts on the ICS. The number of individuals with privileged administrative access to systems is necessary in order to provide a sufficient level of 24/7 support to USBR dams and hydropower plants controlled by the ICS, and to ensure system reliability. In addition, the USBR stated the position descriptions for ICS elevated privilege users contain relevant official duties to include providing technical support, security monitoring, system maintenance, system integration, software administration, testing and implementation, Supervisory Control and Data Acquisition (SCADA) expertise, and serving as a duty officer.

OIG Reply: We disagree that the USBR has implemented least privilege on its ICS. Compliance with least privilege means system administrator access should be limited. As such, the USBR's granting of system administrator privileges to over 50 percent of the ICS user population is inconsistent with the principle of least privilege. In addition, having more user accounts with system administrator rights (30) than ICS users (25) also violates the principle of least privilege. Furthermore, we identified that 9 of the 30 administrator accounts had not been used for a period of one year or more, which does not comply with the least privilege principle.

The USBR's statement regarding 13 of the 25 [redacted] employees with elevated privilege accounts is misleading as it implies that the ICS has over 100 users, rather than 25 users, so the percentage of system users with system administrator appears to be less than the 52 percent we reported. First, it implies a 1 to 1 relationship between system users and system accounts. This is not accurate as some users have multiple accounts and because of group and service accounts. Second, at the time of our evaluation, we requested a complete ICS user listing, which was provided by USBR's chief information security officer. The system-generated list identified 25 active users and 44 active accounts. Moreover, information supplied by the USBR chief information security officer indicated that 13 of the 25 were system administrators. Third, as part of our October 19, 2017 briefing with the USBR we provided in writing our finding related to ICS account practices with USBR staff and they did not dispute that 52 percent of ICS users were granted system administrator access.

Our detailed review of the USBR position designations for the 13 employees with administrator privileges showed that only 5 of the 13 had job functions that required elevated privileges to the ICS. Two of these individuals were supervisory IT specialists, two were IT specialists, and one was an IT Specialist- System Administrator. The other eight employees had engineering or information security roles. Expanding the duties of the eight personnel with engineering and information security roles to also include ICS system administration contradicts the principle of separation of duties, as defined by NIST and recommended industry best practices.

While we acknowledge the need to have 24/7 access, administrator access must be limited to a small subset of users to reduce the risk of insider threats in accordance with NIST and industry best practices. Our interviews with Federal employees from TVA and the U.S. Army Corps of Engineers, who also operate hydropower dams, confirmed the importance of limiting system administrator accounts to a very small number of employees to mitigate risk. Finally, while USBR insists that 13 ICS system users require accounts with administrator privileges, we found that 2 of the 13 individuals had not used their administrator accounts in the last year.

We consider this recommendation unresolved.

2. Eliminate all [redacted] group accounts with elevated privileges and prohibit the use of such accounts in all USBR systems that support Bureau hydroelectric power dams.

   USBR Response: The USBR did not concur with Recommendation 2. The USBR stated that the need for group accounts in SCADA systems is recognized within NIST guidance. The USBR is working with vendors to rewrite many of its applications, but numerous processes require continuous login to a privileged account to function, making shared privileged accounts necessary. The USBR stated that it authorized access to these accounts for 11 system administrators to provide a sufficient level of 24/7 support to dams and hydropower plants and to ensure system reliability. Further, the USBR also stated that it implemented additional compensating controls such as requiring all system administrators to log their use of group accounts, which can then be correlated to physical access records, to include video surveillance and access card use, and the use of these accounts is audited in accordance with NIST guidance. The USBR stated that it implemented shared accounts in accordance with all relevant NIST guidance by identifying the types of system accounts required to support mission functions, establishing conditions for group and role membership, specifically authorizing group and role membership and access authorizations, performing access reviews, and establishing a process for reissuing shared account credentials when individuals are removed. Least privilege has been implemented in accordance with NIST guidance by only authorizing the elevated privileges necessary to accomplish assigned tasks in accordance with mission requirements, and the majority of shared accounts only have access to specific devices. In addition, the USBR has also implemented additional compensating controls in accordance with NIST.

OIG Reply: We disagree with USBR's use of group accounts with elevated privileges, especially since the USBR does not have a logging system that enforces individual accountability by tracing changes made while logged in to a group account back to a specific user, as required by NIST. The use of group accounts with elevated privileges is widely recognized by leading ICS cyber security experts as a poor security practice. Further, this practice is prohibited by the U.S. Army Corps of Engineers. While the USBR insisted that it needs 18 group accounts with privileged access, we found that 7 of the shared accounts had not been used for at least a year.

We disagree with the USBR's assertion that it implemented the principle of least privilege in accordance with NIST guidance. Our review of the 18 shared accounts with elevated privileges showed that 17 have [redacted] full administrative access to all devices and user accounts [redacted] – not limited access to specific devices as indicated in USBR's reply. In addition, two of the shared accounts have [redacted] allow full administrative control over all IT assets and user accounts in the ICS environment. [redacted]

Finally, compensating controls such as video surveillance and access card monitoring are reactive and primarily serve as investigative tools to help assess the severity and extent once a security breach has occurred. Our recommendation is intended to improve security posture by helping prevent security breaches from occurring.

We consider this recommendation unresolved.

3. Implement controls to ensure that ICS user accounts are removed when no longer needed in accordance with DOI policy.

   USBR Response: The USBR partially concurred with Recommendation 3. The USBR stated that it restricted account access to a limited number of devices [redacted]

[redacted] In addition, compensating controls were in place and all but three of the accounts were effectively disabled by other security mechanisms. [redacted] the USBR did not concur that account management procedures should be adhered to throughout the entire system life-cycle and has therefore updated the Access Authorization and Revocation procedure to help ensure compliance in the future.

OIG Reply: While USBR partially concurred with our recommendation, their response did not address the condition identified in our finding, specifically that USBR's practices for actively monitoring accounts with elevated privileges and promptly disabling accounts that had gone unused for 90 or more days as required by its System Security Plan did not occur.

We also found the USBR's statement [redacted] to be inaccurate. A review of the nine privileged accounts which had not been accessed for at least a year showed that eight of the nine accounts had [redacted] full administrative access to all devices and user accounts [redacted] – not access limited to specific devices as indicated in the USBR's response. Finally, the fact that the ICS was undergoing a scheduled change is not relevant as we assessed the ICS environment as it existed at the date of our evaluation.

We reiterate the importance of continuously monitoring user account policies on the ICS because we found that 9 of 30 ICS administrator accounts have not been used for at least a year. Inactive accounts should be removed from the ICS to reduce risk of compromise. Further, not removing the inactive accounts for at least a year indicates failure to monitor ICS user accounts.

We consider this recommendation unresolved.

4. Implement controls to ensure that passwords are regularly changed for ICS user accounts in accordance with DOI policy.

   USBR Response: The USBR partially concurred with Recommendation 4. The USBR cited that the root cause and remediation action for this recommendation is the same as Recommendation 3.

   OIG Reply: While USBR partially concurred with our recommendation, their response did not address the condition identified in our finding.

Specifically, the USBR’s practices for actively monitoring accounts with elevated privileges and promptly disabling accounts that were unused for 90 or more days as required by its System Security Plan did not occur.

We reiterate the importance of continuously monitoring user account policies on the ICS to USBR because we found that 9 of 30 ICS administrator accounts have not been used for at least a year, 10 of 30 administrator accounts had not changed the passwords for at least a year, and 7 of the 18 shared accounts have not been used in at least a year. As stated above, not removing the inactive accounts for at least a year indicates USBR failed to monitor ICS user accounts.

We consider this recommendation unresolved.

5. Establish and implement procedures to ensure additional background scrutiny commensurate with a risk analysis of each employee’s privileges to the ICS and industry best practices.

   USBR Response: The USBR did not concur with Recommendation 5. The USBR stated that according to the Office of Personnel Management (OPM), “Agencies must abide by the standards established by OPM and the Office of the Director of National Intelligence for proper designation of covered positions.” The Reclamation Personnel Security and Suitability policy adheres to all relevant Federal regulations, OPM standards, and the Department of the Interior Position Risk and Sensitivity Designation policy. Position designations are determined by the OPM Suitability Executive Agent Position Designation Tool in accordance with Section 1400.201(b) of Title 5, Code of Federal Regulations, for uniformity and consistency. When using the OPM Position Designation Tool, the required background investigation level for an ICS system administrator is a Tier 2, which aligns with USBR policy.

   OIG Reply: We disagree that the background investigation levels for ICS system administrators are sufficient due to the current environment of escalating threats to critical infrastructure combined with the significant insider threat risk associated with personnel with elevated privileges. The USBR’s personnel security practices prescribe that IT positions with system administrator access to cyber assets supporting critical infrastructure (i.e., ICS) undergo the same background investigation (Tier 2) as IT positions without system administrator access to cyber critical assets. As such, the USBR’s practices do not follow National Security Agency recommendations that personnel with elevated system privileges (i.e., system administrators) undergo more rigorous background investigations to reduce risk. USBR’s personnel security practices also lag behind those of Tennessee Valley Authority and the U.S. Army Corps of Engineers, which require personnel administering and securing the ICS to undergo at least a Tier 3 background investigation and maintain a Secret level security clearance. Finally, the USBR does not benefit from the continuous staff evaluation as defined by 2012 Federal Investigative Standards, because USBR personnel did not have background investigations for the Secret level. Overall, the USBR's response shows that it has not strengthened its personnel security practices in response to the current environment of rapidly escalating threats to industrial control systems.

OPM's Position Designation Tool is a resource that helps government officials determine the appropriate designation, background check and security clearance level for Federal positions. The output can be adjusted up or down by management depending on risk factors such as the duties, roles, and responsibilities of the position. A person in a position with full administrative authority over an ICS that operates critical infrastructure has a much higher risk rating than a non-privileged ICS user. Accordingly, that person should undergo a more rigorous background investigation as a measure to reduce insider threat risk.

We consider this recommendation unresolved.

Appendix 1: Scope and Methodology

Scope

The objective of this evaluation was to assess the effectiveness of the U.S. Bureau of Reclamation's (USBR's) security controls for systems that operate and control its dams. We performed technical testing of the related computer networks, industrial control systems, and business systems.

For this evaluation, our work was limited to the business system and the industrial control system that operate, manage, and support two of its hydropower dams categorized as critical infrastructure.

Methodology

To accomplish our evaluation objective, we:

- Reviewed system security policies and procedures
- Conducted interviews with personnel at the USBR Operations Center
- Performed a walkthrough of the dams
- Obtained network traffic and random access memory (RAM) data from a third party for our analysis
- Developed a system inventory based on network traffic to determine whether USBR has a complete IT asset inventory for the ICS and then compared it to the inventory provided by the USBR
- Analyzed network traffic on business and industrial control systems for the presence of malware and other indicators of compromise
- Analyzed RAM captures for the presence of malware or other indicators of compromise
- Obtained and reviewed current user listings, position descriptions, and background investigation and clearance levels for users with administrator privileges
- Consulted with employees at the Tennessee Valley Authority (TVA) and the U.S. Army Corps of Engineers (USACE) who are responsible for overseeing or managing hydropower operations to determine their account management and personnel security practices

- Consulted with leading industrial control system cybersecurity experts at the SysAdmin, Audit, Network, and Security (SANS) Institute

We assessed selected controls based on risk, including account management and personnel security for both the business and control systems that support the dams. We also reviewed NIST SP-800-53 Rev. 4 *Security and Privacy Controls for Federal Information Systems and Organizations*, dated April 2013, and NIST SP 800-82 Rev. 2, *Guide to Industrial Control System Security*," dated May 2015.

As part of our technical testing, we conducted interviews with the operations center and dam staff from April 17 through April 20, 2017. We obtained network traffic samples from a third party for the business and control system environments for the dams.

To facilitate asset discovery across both the business and control systems supporting the dams, we used the GRASSMARLIN tool developed by the National Security Agency as well as the CyberLens® tool. GRASSMARLIN enabled our team to passively map and visually display a network topology, while safely conducting device discovery, accounting, and reporting on these critical cyber-physical systems. In addition, we were able to validate open ports and services through network packet inspection. We used the CyberLens® tool for its robust reporting capabilities to develop an inventory of systems based on network packet capture files to validate the completeness and accuracy of the inventory of assets attached to the network.

We analyzed network traffic data, using open-source based tools, including Suricata and Bro, to identify any indicators of compromise (artifacts observed on a network or operating system that with high confidence indicate a computer intrusion may have occurred). Suricata is an intrusion detection system (IDS). It has a complete signature language to match on known threats, policy violations, and malicious behavior. It will detect many anomalies in the traffic that it inspects. To further enhance the capabilities of the tool, we used an enhanced malware ruleset for packet inspection to determine the presence of any malware. In addition, we used Bro to help detect and identify the presence of malware, a powerful network analysis tool that is both a signature and anomaly-based IDS. Its analysis engine can convert captured network traffic into a series of events that we used with its own scripting language.

Operations performed on a computing device by both legitimate users and adversaries modify the device's RAM, leaving evidence of on the device. Memory forensics is an integral part of threat hunting and involves acquiring RAM off network devices, then analyzing its contents to identify artifacts that may indicate compromise, such as malicious code and processes, and abnormal network connections. It also can assess the impact of the compromise on the network. As part of our technical testing, we obtained 150 gigabytes of RAM from 12 computer servers and workstations that operate and control the dams.

Using Volatility, an open source collection of tools for the extraction of digital artifacts from RAM, we analyzed the RAM for the presence of malware on the ICS network.

To assess account management controls, we obtained current user listings to determine if access was provisioned correctly following the least privilege principle and if duties were adequately segregated. For in-scope systems, we assessed the entire population of users with administrator privileges. We also reviewed the position descriptions, as well as background investigation and clearance levels for all administrator users to assess whether individuals with elevated privileges undergo more rigorous background investigations to mitigate risk.

To benchmark cybersecurity practices for ICS, we met with personnel at other Federal agencies that oversee and maintain hydropower dams in the United States, including the TVA and USACE. Personnel at these agencies provided insights on leading best practices for account management for industrial control systems that operate and control dams.

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

Appendix 2: Response to Draft Report

The U.S. Bureau of Reclamation's response to our draft report follows on page 22.

United States Department of the Interior

BUREAU OF RECLAMATION
Washington, DC 20240

IN REPLY REFER TO:

84-27410
3.1.03

VIA ELECTRONIC MAIL ONLY

MEMORANDUM

To: Office of Inspector General
Attn: Assistant Inspector General for Audits,
Inspections, and Evaluations

Through: Timothy R. Petty, Ph.D.
Assistant Secretary
for Water and Science

Timothy R. Petty

MAR 16 2018

From: Brenda Burman
Commissioner

MAR 12 2018

Subject: The Bureau of Reclamation's Response to the Office of Inspector General (OIG) Management Advisory, U.S. Bureau of Reclamation Selected Hydropower Dams at Increased Risk from Insider Threats, Report No. 2017-ITA-023

The OIG, in its January 25, 2018, Draft Evaluation Report, *U.S. Bureau of Reclamation Selected Hydropower Dams at Increased Risk for Insider Threats*, requested that Reclamation inform the OIG of the planned course of action to address and implement the recommendations in the subject report. The requested information is attached.

If you have any questions or require additional information, please contact Elizabeth Cordova-Harrison, Director, Mission Support Organization, at 303-445-2783.

Attachment

cc: Chief Information Officer
Attn: Sylvia Burns
ASWS
Attn: Kerry Rae
94-00000 (GPayne, AShepet)
84-27000 (SDeMarco Reading File), 84-27400 (Reading File), 84-27410 (AHartman),
84-21000 (KSmiley), 84-21220 (CGarcia, DGaspar, JHarris, RStevens)
(w/att to each)

Attachment

The Bureau of Reclamation's Response to the Office of Inspector General (OIG) Draft Evaluation Report U.S. Bureau of Reclamation Selected Hydropower Dams at Increased Risk from Insider Threats, Report No. 2017-ITA-023

January 2018

General Comments: [redacted]

[redacted]

Response to OIG Recommendations

Recommendation 1: Implement "least privilege" by limiting the number of USBR employees with elevated privileges to [redacted] based on the official duties listed in their respective position designations.

> Reclamation's Response: Non-concur. The [redacted] has implemented least privilege in accordance with National Institutes of Standards and Technology (NIST) guidance by only authorizing the elevated privileges necessary to accomplish assigned tasks in accordance with mission requirements. Elevated privileges

are only granted to Reclamation employees who administer the system or network, provide technical support or perform cybersecurity-related functions. Thirteen of the 25 [redacted] employees (52 percent) do have elevated privilege accounts since [redacted] is responsible for providing system operations and maintenance for the entire [redacted] system, but that percentage is not representative for the system as a whole, since there are over 100 active accounts on [redacted]. The number of individuals with privileged administrative access to systems is necessary in order to provide a sufficient level of 24/7 support to Reclamation dams and hydropower plants controlled by [redacted], and to ensure system reliability. In addition, the position descriptions for [redacted] elevated privilege users do contain relevant official duties to include providing technical support, security monitoring, system maintenance, system integration, software administration, testing and implementation, Supervisory Control and Data Acquisition (SCADA) expertise, and serving as a duty officer. Per the Office of Personnel and Management (OPM), a position description "documents the major duties, responsibilities and organizational relationships of a job." OPM further states that "it is not necessary to detail the specific steps needed to carry out a duty," therefore specific references to the names of systems and/or the type of logical access required on those systems, are typically not documented in a Position Description. The authorization for elevated privileges is documented using the [redacted] user account access request form in accordance with [redacted] account management procedures.

Responsible Official: Karla Smiley, Associate Chief Information Officer (ACIO)

Target Implementation Date: Not applicable.

Recommendation 2: Eliminate all [redacted] group accounts with elevated privileges and prohibit the use of such accounts in all USBR systems that support Bureau hydroelectric power dams.

Reclamation's Response: Non-concur. The need for group accounts in SCADA systems is well recognized within National Institute for Standards and Tehcnology (NIST) guidance. The [redacted] is working with vendors to rewrite many of their applications, however currently there are numerous processes that require a continuously logged in privileged account to function, making shared privileged accounts necessary. The [redacted] has authorized 11 system administrators to have access to these accounts in order to provide a sufficient level of 24/7 support to Reclamation dams and hydropower plants controlled by [redacted], and to ensure system reliability. As a compensating control, the [redacted] requires all system administrators to log their use of group accounts, which can then be correlated to physical access records, to include video surveillance and access card use, and the use of these accounts is audited in accordance with NIST guidance. The [redacted] has implemented shared accounts in accordance with all relevant NIST guidance by identifying the types of system accounts required to support mission functions, establishing conditions for group and role membership, specifically authorizing group and role membership and access authorizations, performing access reviews, and establishing a process for reissuing shared account credentials when individuals are removed. Least privilege has been implemented in accordance with NIST guidance by only authorizing the elevated privileges necessary to accomplish assigned tasks in accordance with mission requirements, and the majority of shared accounts only have access to specific devices. In addition, the [redacted] has also implemented additional compensating controls in accordance with NIST Special Publication (SP) 800-82, *Guide to Industrial Control System (ICS) Security* and the environment is monitored by a Security Information and Event Management system that logs all account authentication requests and alerts on multiple failed authentication attempts. Audit logs are protected from modification or deletion and are reviewed and retained in accordance with all relevant requirements. The NIST security control that requires unique identification of organizational users, IA-02, does not apply to the authorized use of group authenticators without individual authentication and IA-02 control enhancement 5, requiring individuals to be authenticated with an individual authenticator when a group authenticator is employed, is not required for any federal system according to the security control baselines identified in NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*.

Responsible Official: Karla Smiley, Associate Chief Information Officer (ACIO)

Target Implementation Date: Not applicable.

Recommendation 3: Implement controls to ensure that ICS user accounts are removed when no longer needed in accordance with DOI policy.

Reclamation's Response: Partially concur. [redacted] In addition, compensating controls were in place and all but three of the accounts were effectively disabled by other security mechanisms. [redacted] does concur that account management procedures should be adhered to throughout the entire system life-cycle and has therefore updated the [redacted] Access Authorization and Revocation procedure to help ensure compliance in the future.

Responsible Official: Karla Smiley, Associate Chief Information Officer (ACIO)

Target Implementation Date: Completed 2/7/2018.

Recommendation 4: Implement controls to ensure that passwords are regularly changed for ICS user accounts in accordance with DOI policy.

Reclamation's Response: Partially concur, see response for Recommendation 3. The root cause of the identified issues and the remediation action is the same for both recommendations.

Responsible Official: Karla Smiley, Associate Chief Information Officer (ACIO)

Target Implementation Date: Completed 2/7/2018.

Recommendation 5: Establish and implement procedures to ensure additional background scrutiny commensurate with a risk analysis of each employee's privileges to the ICS and industry best practices.

Reclamation's Response: Non-concur. Per OPM, "Agencies must abide by the standards established by OPM and the Office of the Director of National Intelligence for proper designation of covered positions." Reclamation Personnel Security and Suitability policy adheres to all relevant federal regulations, OPM standards, and the Department of the Interior Position Risk and Sensitivity Designation policy. Position designations are determined by the OPM Suitability Executive Agent Position Designation Tool in accordance with Section 1400.201(b) of Title 5, Code of Federal Regulations, for uniformity and consistency. As demonstrated when using the OPM Position Designation Tool, the required background investigation level for a [redacted] system administrator is a Tier 2, which aligns with Reclamation policy.

Responsible Official: Karla Smiley, Associate Chief Information Officer (ACIO)

Target Implementation Date: Not applicable.

Appendix 3: Status of Recommendations

In response to our draft report, the U.S. Bureau of Reclamation (USBR) partially concurred with two recommendations and did not concur with three recommendations. The USBR's response to our draft report is included in Appendix 2. Based on this response, we consider all five recommendations unresolved. We will forward them to the Office of Policy, Management and Budget for resolution and to track their implementation.

Recommendations	Status	Action Required
1 - 5	Unresolved	We will refer these recommendations to the Assistant Secretary for Policy, Management and Budget for resolution.

Report Fraud, Waste, and Mismanagement

Fraud, waste, and mismanagement in Government concern everyone: Office of Inspector General staff, departmental employees, and the general public. We actively solicit allegations of any inefficient and wasteful practices, fraud, and mismanagement related to departmental or Insular Area programs and operations. You can report allegations to us in several ways.

By Internet:	www.doioig.gov	
By Phone:	24-Hour Toll Free:	800-424-5081
	Washington Metro Area:	202-208-5300
By Fax:	703-487-5402	

By Mail:

U.S. Department of the Interior
Office of Inspector General
Mail Stop 4428 MIB
1849 C Street, NW.
Washington, DC 20240