

~~FOR OFFICIAL USE ONLY~~

Report No. DODIG-2013-036

January 14, 2013

Inspector General

United States
Department of Defense



Improvements Are Needed to Strengthen the
Security Posture of USACE, Civil Works, Critical
Infrastructure and Industrial Control Systems in the
Northwestern Division

~~This document contains information that
may be exempt from mandatory disclosure
under the Freedom of Information Act.~~

~~FOR OFFICIAL USE ONLY~~

Additional Copies

To obtain additional copies of this report, contact the Secondary Reports Distribution Unit at (703) 604-8937 (DSN 664-8937) or fax (703) 604-8932.

Suggestions for Audits

To suggest or request audits, contact the Office of the Deputy Inspector General for Auditing at auditnet@dodig.mil or by mail:

Department of Defense Office of Inspector General
Office of the Deputy Inspector General for Auditing
ATTN: Audit Suggestions/13F25-04
4800 Mark Center Drive
Alexandria, VA 22350-1500



Acronyms and Abbreviations

DISA	Defense Information Systems Agency
GDACS	Generic Data Acquisition Control System
IA	Information Assurance
IAVA	Information Assurance Vulnerability Alert
ICS	Industrial Control System
IDS	Intrusion Detection System
MEVA	Mission Essential or Vulnerable Area
NIST SP	National Institute of Standards and Technology Special Publication
OPM	Operations Project Manager
PLC	Programmable Logic Controller
SCADA	Supervisory Control and Data Acquisition
STIG	Security Technical Implementation Guide
USACE	U.S. Army Corps of Engineers



INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
4800 MARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22350-1500

January 14, 2013

MEMORANDUM FOR ASSISTANT SECRETARY OF THE ARMY
FOR CIVIL WORKS
DIRECTOR OF CIVIL WORKS, U.S. ARMY CORPS
OF ENGINEERS
AUDITOR GENERAL, DEPARTMENT OF THE ARMY

SUBJECT: Improvements Are Needed to Strengthen the Security Posture of USACE, Civil Works, Critical Infrastructure and Industrial Control Systems in the Northwestern Division (Report No. DODIG-2013-036)

We are providing this report for your review and comment. The Commanders and District Engineers, Portland and Seattle Districts; Operations Project Managers for (b)(3) 10 USC 130e (USACE)

and the Chief, Hydroelectric Design Center did not consistently and adequately protect critical infrastructure and the industrial control systems used to operate those structures from unauthorized access. We considered USACE comments on a draft of this report when preparing the final report.

DoD Directive 7650.3 requires that recommendations be resolved promptly. As a result of management comments, we revised draft Recommendations A.1.a, A.1.c, A.3, A.6.a.(1), A.6.a.(3), A.6.b, B.1, B.2.a, and B.2.c and deleted draft Recommendation A.6.a.(4). Comments from the Chief, Operations Division, USACE, Civil Works, on Recommendations A.1.a, A.1.b, A.1.c, A.1.d, A.2.b, A.4.b, A.5.b, A.6.a.(1), A.6.a.(2), A.6.a.(3), B.2.a, B.2.b, B.3.a.(1), B.3.a.(2), B.3.a.(3), B.3.a.(4), B.3.a.(5), B.3.b, B.3.c, B.3.d, B.3.e, B.4.b, B.4.c, B.5, B.7.b, and C were responsive and generally conformed to the requirements of DoD Directive 7650.3. The Chief, Operations Division, comments on Recommendations A.2.a, A.3, A.4.a, A.5.a, A.6.b, B.1, B.2.c, B.4.a, B.6, and B.7.a were partially responsive, and comments on Recommendations B.8 were nonresponsive. Therefore, we request that the Chief, Operations Division, provide additional comments on those recommendations by February 13, 2013.

If possible, send a portable document format (.pdf) file containing your comments to audros@dodig.mil. Pdf copies of your comments must have the actual signature of the authorizing official for your organization. We are unable to accept the /Signed/ symbol in place of the actual signature. If you arrange to send classified comments electronically, you must send them over the SECRET Internet Protocol Router Network (SIPRNET).

We appreciate the courtesies extended to the staff. Please direct questions to me at (703) 604-8866 (DSN 664-8866).

Alice F. Carey
Assistant Inspector General
Readiness, Operations, and Support



Results in Brief: Improvements Are Needed to Strengthen the Security Posture of USACE, Civil Works, Critical Infrastructure and Industrial Control Systems in the Northwestern Division

What We Did

We determined whether U.S. Army Corps of Engineers (USACE), Civil Works, personnel implemented effective procedures and security controls over critical infrastructure to protect against unauthorized access from physical and cyber threats that affect information systems used to operate water control structures.

What We Found

Overall, the Operations Project Managers (OPMs) for the five projects did not consistently implement physical security controls and 17 of 26 information assurance (IA) controls to secure and protect critical infrastructure and industrial control systems (ICSs) against unauthorized access from physical and cyber threats. See Appendix B for a discussion of the IA controls that we tested and the results of our review.

~~(FOUO)~~ Although the OPMs for 2 of the 5 projects effectively implemented the 11 physical security requirements to detect and protect against unauthorized access, the OPMs for 3 projects did not. In particular, OPMs did not implement

(b)(3) 10 USC 130e (USACE)
(b)(3) 10 USC 130e (USACE)

(b)(3) 10 USC 130e (USACE)

~~(FOUO)~~ These weaknesses existed because the Commanders and District Engineers, Portland

~~(FOUO)~~ and Seattle Districts, and the OPMs did not generally recognize the criticality of physical security shortfalls when prioritizing funding. Also, the physical security requirements were not implemented a

(b)(3) 10 USC 130e (USACE)

(b)(3) 10 USC 130e (USACE)

(b)(3) 10 USC 130e (USACE)

(b)(3) 10 USC 130e (USACE)

~~(FOUO)~~ (b)(3) 10 USC 130e (USACE)

Also, the Commanders and District Engineers did not appoint, in writing, in accordance with DoD requirements, the personnel performing IA

~~(FOUO)~~ responsibilities. They stated they did not know all positions required appointments.

~~(FOUO)~~ (b)(3) 10 USC 130e (USACE)

(b)(3) 10 USC 130e (USACE)

(b)(3) 10 USC 130e (USACE)

~~(FOUO)~~ (b)(3) 10 USC 130e (USACE)

~~(FOUO)~~ In addition, we recommend that the Chief, Hydroelectric Design Center, conduct more frequent vulnerability assessments. We also recommend that the Deputy Chief of Engineers, USACE, monitor the status of certification and accreditation actions through plans of action and milestones. Further, we recommend that the USACE, Programs Division, revise the current budget process to separately identify IA requirements for the protection of the information systems used to operate critical infrastructure from cyber security risks.

Management Comments and Our Response

On the basis of management comments, we revised nine recommendations to clarify the intent of our recommendations related to implementing physical security and conducting penetration testing. We also deleted a recommendation on the basis of management comments because the required actions could not be completed. Comments from USACE were generally responsive; however, some comments were partially responsive or nonresponsive to the intent of our recommendations.

We request that management provide additional comments by February 13, 2013. Please see the Recommendations Table on the next page.

What We Recommend

~~(FOUO)~~ We recommend that the Commanders and District Engineers, Portland and Seattle Districts, in coordination with the OPMs, implement required physical security measures in accordance with requirements defined in the USACE, "Baseline Security Posture Guide for Civil Works Projects;" (b)(3) 10 USC 130e (USACE)

Recommendations Table

Management	Recommendations Requiring Comment or Planned Completion Date	No Additional Comments Required
Commander and District Engineer, Portland District, U.S. Army Corps of Engineers	A.1.a, A.1.b, A.1.c, A.1.d, A.2.a, A.2.b, A.3, B.4.a, B.5, B.6, B.8	B.4.b, B.4.c
Commander and District Engineer, Seattle District, U.S. Army Corps of Engineers	A.4.a, A.5.a, A.5.b, A.6.a.(1), A.6.a.(2), A.6.a.(3), A.6.b, B.3.a.(1), B.3.a.(2), B.3.a.(3), B.3.a.(4), B.3.a.(5), B.3.b, B.3.c, B.3.d, B.3.e, B.7.a, B.7.b, B.8	A.4.b
Chief, Hydroelectric Design Center, U.S. Army Corps of Engineers	B.2.c	B.2.a, B.2.b
U.S. Army Corps of Engineers, Programs Integration Division	B.1	
Deputy Chief of Engineers, U.S. Army Corps of Engineers	C	

Please provide comments or the planned completion date by February 13, 2013.

Table of Contents

Introduction	1
Objective	1
Background on USACE Operations and Critical Infrastructure	1
Identification and Prioritization	
Review of Internal Controls	6
(FOUO) Finding A. (b)(3) 10 USC 130e (USACE)	7
(b)(3) 10 USC 130e (USACE)	
(b)(3) 10 USC 130e (USACE)	7
(b)(3) 10 USC 130e (USACE)	14
Recommendations, Management Comments, and Our Response	14
Finding B. (b)(3) 10 USC 130e (USACE)	24
(b)(3) 10 USC 130e (USACE)	
(b)(3) 10 USC 130e (USACE)	25
(b)(3) 10 USC 130e (USACE)	37
Conclusion	42
Recommendations, Management Comments, and Our Response	43
Finding C. (b)(3) 10 USC 130e (USACE)	55
(b)(3) 10 USC 130e (USACE)	55
(b)(3) 10 USC 130e (USACE)	
(b)(3) 10 USC 130e (USACE)	56
(b)(3) 10 USC 130e (USACE)	
Recommendations, Management Comments, and Our Response	57
Appendices	
A. Scope and Methodology	58
Use of Computer-Processed Data	60
Use of Technical Assistance	60
Prior Coverage	60
B. IA Controls Reviewed	61
C. USACE Comments on the Findings and Our Response	67
Glossary	76
Management Comments	
U.S. Army Corps of Engineers	79

Introduction

Objective

Our objective was to determine whether U.S. Army Corps of Engineers (USACE), Civil Works, personnel implemented effective procedures and security controls over critical infrastructure to protect against unauthorized access to information systems that support water control structures from physical and cyber threats. See Appendix A for a discussion of the scope and methodology related to the audit objective. See the Glossary for terms used throughout the report.

Background on USACE Operations and Critical Infrastructure Identification and Prioritization

USACE is responsible for providing engineering services in peace and war to strengthen our Nation's security, support the economy, and reduce risks from disasters. The USACE, Civil Works Directorate, is responsible for providing water resource services, including emergency response, for water resource development activities supporting hydropower generation, flood control, navigation, recreation, and infrastructure and environmental stewardship. USACE operates 702 water structures; approximately 556 of those structures primarily control flooding and 75 generate hydropower. USACE provides services through its 45 districts that are subordinate to 9 divisions.

Northwestern Division and Portland and Seattle District Responsibilities

We reviewed information assurance (IA) and physical security controls over three information systems used to operate five Portland and Seattle District projects in the Northwestern Division. The Northwestern Division is one of nine USACE divisions and is responsible for providing engineering services and stewardship of water resource infrastructure, military construction, environmental protection and restoration, and emergency response operations. The Northwestern Division performs its responsibilities through resources managed by the Portland, Seattle, Walla Walla, Omaha, and Kansas City Districts.

The Portland District is responsible for providing vital public engineering services to the Pacific Northwest to strengthen security, promote a strong economy, and enhance environmental sustainability by:

- improving and maintaining navigation for economic development and safety,
- preventing and reducing flood damage,
- generating reliable and efficient hydropower,
- supporting combat, stability, and disaster operations through forward-deployed and reachback capabilities,
- providing Corps-wide expertise in hydroelectric planning and engineering, and
- providing safe and healthful recreational opportunities for the public.

The Seattle District plans, designs, and builds flood risk management, navigation, water supply, and ecosystem restoration projects. Specifically, the Seattle District plans, designs, constructs, operates, and maintains flood control projects; and operates three hydropower projects.

Portland and Seattle District Projects and Industrial Control Systems Reviewed

We visited (b)(3) 10 USC 130e (USACE) in the Portland District as well as (b)(3) 10 USC 130e (USACE) in the Seattle District (the five projects). The Portland District is comprised of 19 structures; each of the structures is operated by an industrial control system (ICS). National Institute of Standards and Technology, Special Publication (NIST SP) 800-82, "Guide to Industrial Control Systems (ICS) Security," June 2011, states that an ICS includes supervisory control and data acquisition (SCADA)¹ systems, distributed control systems, and programmable logic controllers (PLC).² In general, an ICS supports the industrial sector and critical infrastructure.

Overall, the Portland District has three groups of projects within the Willamette Valley, Columbia River Basin, and Rogue River Basin. (b)(3) 10 USC 130e (USACE) Dam are part of the Willamette Valley, and (b)(3) 10 USC 130e (USACE) is part of the (b)(3) 10 USC 130e (USACE). Figures 1 and 2 show the (b)(3) 10 USC 130e (USACE), respectively.



Source: USACE Northwestern Division Website

Source: DoD Office of Inspector General

~~(FOUO)~~ The 13 projects in the Willamette Valley, including (b)(3) 10 USC 130e (USACE) and (b)(3) 10 USC 130e (USACE). Three of the four projects along the Columbia River Basin (b)(3) 10 USC 130e (USACE).

¹ NIST SP 800-82 defines a SCADA system as a highly distributed system used to control geographically dispersed assets.

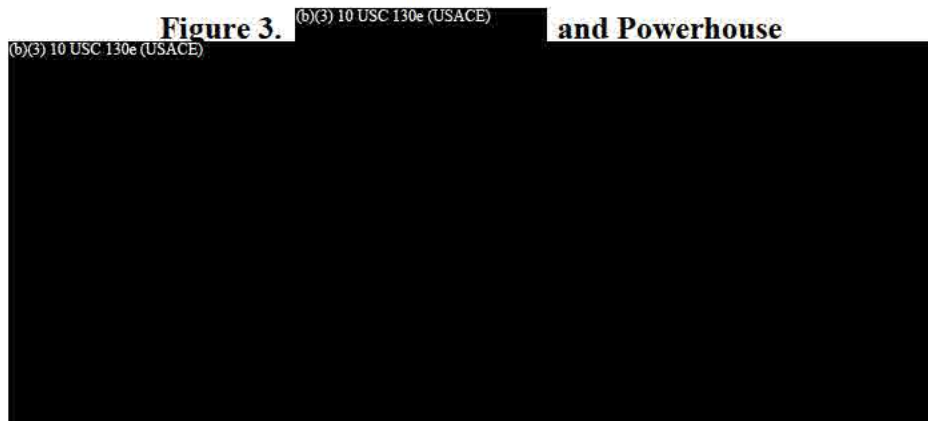
² NIST SP 800-82 defines a PLC as a solid-state control system that has a user-programmable memory for storing instructions for implementing specific functions (for example, input and output control and communications).

(FOUO) (b)(3) 10 USC 130e (USACE). The North American Electric Reliability Corporation designated the projects along the Columbia River Basin as bulk electric producing projects.³ We did not review the ICS used by the two projects along the Rogue River Basin.

(FOUO) The Seattle District is comprised of five water control structures, three of which use an ICS for operating the structures. In particular, two projects were built primarily to control flooding, while the remaining three projects were built primarily to generate hydropower. (b)(3) 10 USC 130e (USACE), which provides flood control, (b)(3) 10 USC 130e (USACE)

whereas, (b)(3) 10 USC 130e (USACE), which generates hydropower, (b)(3) 10 USC 130e (USACE) was also designated as a bulk electric-producing project. The two remaining hydropower projects in the Seattle District are (b)(3) 10 USC 130e (USACE), (b)(3) 10 USC 130e (USACE)

(b)(3) 10 USC 130e (USACE) Figure 3 shows (b)(3) 10 USC 130e (USACE)



Source: DoD Office of Inspector General

Identification and Prioritization of USACE Critical Infrastructure

(FOUO) Headquarters, USACE, Office of Homeland Security, is responsible for emergency management, flood management, and critical infrastructure management programs. On January 4, 2002, Headquarters, USACE, established the Critical Project Security Program⁴ to assess and improve the security posture of Corps-owned water infrastructure following the terrorist attacks of September 11, 2001. This Program focused on developing a risk-based prioritized list of Corps projects that needed physical security upgrades to protect them against terrorist threats. The USACE Office of Homeland Security conducted physical security assessments between 2002 and 2004; these assessments were known as the risk assessment methodology for dams. The assessments resulted in the identification of 263 critical infrastructure projects, including

³ The North American Electric Reliability Corporation, an electric reliability organization certified by the Federal Energy Regulatory Commission, requires bulk electric projects to meet 107 critical infrastructure protection standards, 8 of which pertain to protecting information systems from cyber security attacks.

⁴ In early 2004, the Critical Project Security Program evolved into the Critical Infrastructure Security Program to encompass all USACE, Civil Works, projects.

(FOUO)

(b)(3) 10 USC 130e (USACE)

The assessments also resulted in USACE implementing security requirements at 85 of those projects, including (b)(3) 10 USC 130e (USACE) and (b)(3) 10 USC 130e (USACE)

(b)(3) 10 USC 130e (USACE)

(b)(3) 10 USC 130e (USACE)

(FOUO)

(b)(3) 10 USC 130e (USACE)

Homeland Security Presidential Directive-7, "Critical Infrastructure Identification, Prioritization, and Protection," December 17, 2003, requires Federal agencies to identify, prioritize, and protect critical infrastructure from terrorist attacks. It also requires the Secretary of Homeland Security to develop a comprehensive plan for assessing the Nation's critical infrastructure. As a result, the Secretary of Homeland Security developed the National Infrastructure Protection Plan to provide an overarching framework for integrating the Nation's critical infrastructure and key resource protection initiatives into a single, national effort. The National Infrastructure Protection Plan identifies 18 overall sectors affecting the Nation's critical infrastructure; one of which is the Dams sector, led by the Department of Homeland Security.

The Secretary of Homeland Security, in coordination with other Dams sector partners, developed the Dams Sector-Specific Plan to establish sectorwide processes for identifying and prioritizing assets, assessing risk within the sector, implementing protective programs and resilience strategies, and measuring the effectiveness of those

programs and strategies. The Dams sector includes dams, hydropower generation facilities, navigation locks, levees, dikes, hurricane barriers, and other similar water retention and water control facilities. The Plan states that dams are complex facilities that may include multiple water impoundment or control structures, reservoirs, spillways, outlet works, powerhouses, canals or aqueducts, and in some cases, navigation locks.

~~(FOUO)~~ In 2009, the USACE Critical Infrastructure Security Program became the USACE Critical Infrastructure Protection and Resilience Program to address policy requirements outlined by HSPD-7 and responsibilities as a Federal owner and operator of critical infrastructure. Under this program, the USACE Office of Homeland Security began evaluating the criticality of all USACE dams using an agreed-upon methodology that all Federal, State, and local governments, and private and public partners within the Dams sector use. The overall assessment evaluates potential human, economic, and mission impacts based on a list of Department of Homeland Security criteria. As of March 2012, the USACE Office of Homeland Security completed its evaluation of 170 structures, 124 of which it designated as critical infrastructure. Those results showed overall USACE-wide criticality rankings (most to least) as follows:

- ~~(FOUO)~~
- ~~(FOUO)~~
- ~~(FOUO)~~
- ~~(FOUO)~~
- ~~(FOUO)~~

(b)(3) 10 USC 130e (USACE)



In 2011, the USACE Critical Infrastructure Protection and Resilience Program worked with the Institute of Defense Analysis to develop the common risk model for dams to support Corps-wide risk assessments and asset prioritization based on land-based, waterside, and airborne risk scenarios. The design and implementation of physical security measures were to be based on specific risks to each project. According to the Program Manager, USACE Critical Infrastructure Protection and Resilience Program, 18 projects were assessed under the common risk model for dams, including all 5 projects we visited.

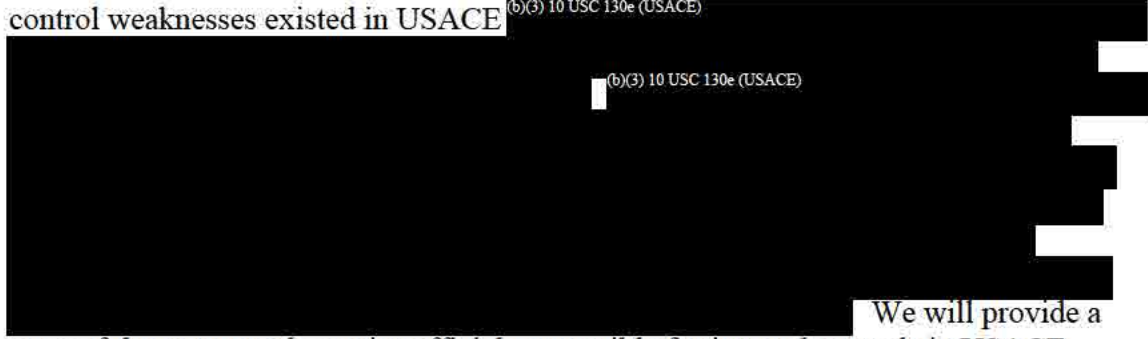
Information Assurance and Physical Security Requirements

DoD Instruction (DoDI) 8500.2, "Information Assurance (IA) Implementation," February 6, 2003, establishes a baseline level of IA controls for all DoD information systems by requiring system owners to assign each system a mission assurance category and confidentiality level. The USACE Information Assurance Program Manager stated that USACE generally designated all ICS networks used to operate hydropower generation projects as mission assurance category II networks that processed sensitive information. Therefore, USACE personnel were responsible for the design and implementation of IA controls to provide integrated, layered protection of each ICS. We reviewed 26 of 107 DoDI 8500.2 IA controls to determine whether the implementation of those controls was effective to prevent unauthorized physical and cyber-related access to the ICSs used to operate USACE-designated critical infrastructure. See Appendix B for the list of DoDI 8500.2 controls we reviewed.

Army Regulation 190-13, "The Army Physical Security Program," February 25, 2011, prescribes policy and assigns responsibility for developing and maintaining practical, economical, and effective physical security programs. The Regulation requires commanders to designate, in writing, mission essential or vulnerable areas (MEVAs); designate restricted areas; install intrusion detection systems; maintain daily records of intrusion detection system alarms and malfunctions; and implement minimum uniform standards and procedures for controlling personnel movement into, and movement within, restricted areas.

Review of Internal Controls

~~(FOUO)~~ DoDI 5010.40, "Managers' Internal Control Program (MICP) Procedures," July 29, 2010, requires DoD organizations to implement a comprehensive system of internal controls that provides reasonable assurance that programs are operating as intended and to evaluate the effectiveness of the controls. We determined that internal control weaknesses existed in USACE (b)(3) 10 USC 130e (USACE)



(b)(3) 10 USC 130e (USACE)

We will provide a copy of the report to the senior official responsible for internal controls in USACE.

(FOUO) Finding A.

(b)(3) 10 USC 130e (USACE)

(b)(3) 10 USC 130e (USACE)

(b)(3) 10 USC 130e (USACE)

(FOUO)

(b)(3) 10 USC 130e (USACE)

(b)(3) 10 USC 130e (USACE)

(b)(3) 10 USC 130e (USACE)

Physical Security Was Not Always Sufficient or Effective

(FOUO)

(b)(3) 10 USC 130e (USACE)

(b)(3) 10 USC 130e (USACE)

(b)
(3)
10
US

⁵ The USACE “Baseline Security Posture Guide for Civil Works Projects” includes 14 Baseline Security Posture level II requirements; however, we reported on only 11 of those requirements that pertained to detecting and protecting projects against unauthorized access. The three requirements we did not report on include posted signs, site security plans, and site recovery plans.

USACE Baseline Security Posture Requirements Were Not Effectively Implemented

The OPMs for (b)(3) 10 USC 130e (USACE) did not always implement all 11 security requirements designed to detect and to protect against unauthorized access. The “Baseline Security Posture Guide” requires District Commanders to assess the likelihood of an attack, potential damages to the project, and the probable loss of life and economic impact for determining which overall Baseline Security Posture to implement. The Commanders and District Engineers, Portland and Seattle Districts, evaluated and designated (b)(3) 10 USC 130e (USACE) as structures required to implement Baseline Security Posture level II requirements. (b)(3) 10 USC 130e (USACE)

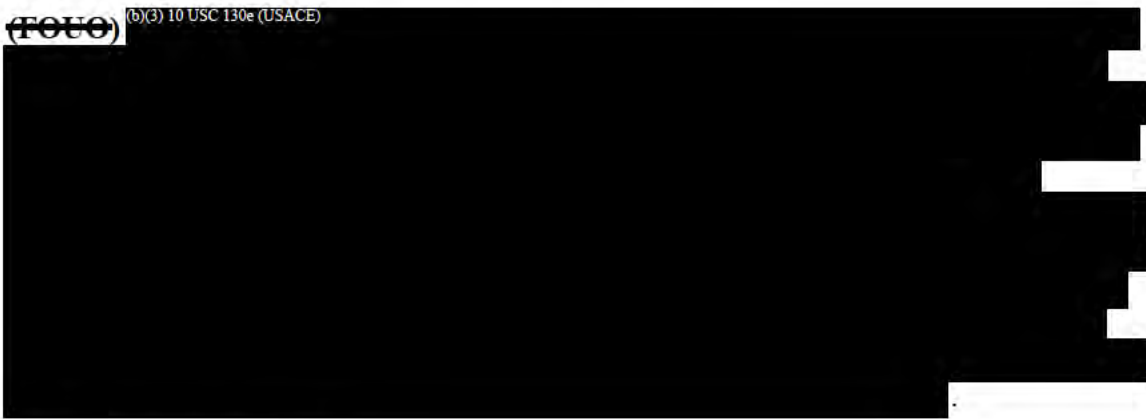
(b)(3) 10 USC 130e (USACE)

~~(FOUO)~~ Table 1. Implementation of Baseline Security Posture Requirements

	Baseline Security Posture Level II Requirements	(b)(3) 10 USC 130e (USACE)
1	(b)(3) 10 USC 130e (USACE)	
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		


(FOUO)

(b)(3) 10 USC 130e (USACE)




(FOUO)

(b)(3) 10 USC 130e (USACE)

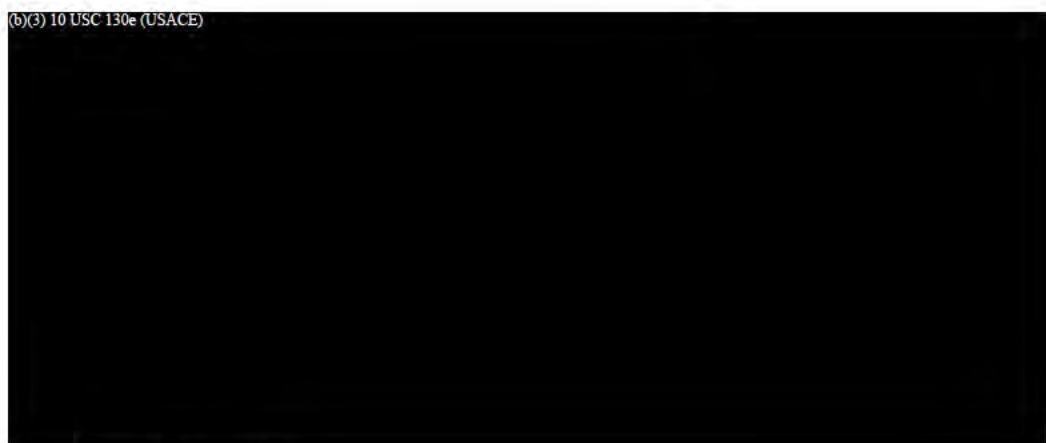


(FOUO)

(b)(3) 10 USC 130e (USACE)




(b)(3) 10 USC 130e (USACE)



(FOUO)

(b)(3) 10 USC 130e (USACE)



(FOUO)

(b)(3) 10 USC 130e (USACE)

The OPMs for (b)(3) 10 USC 130e (USACE) generally thought their structures were secure; however, an intruder compromised physical security at (b)(3) 10 USC 130e (USACE) on March 2, 2011, by jumping a barbed wire fence. Although the physical security measures at (b)(3) 10 USC 130e (USACE) immediately notified the operator on duty of the breach and began capturing video of the incident, it took local law enforcement approximately (b)(3) minutes to respond because of the remote location of this structure. During the incident, the intruder was captured on video taking pictures of the structure from the topside of the dam.⁶

Terrorist and criminal acts are often preceded by reconnaissance activities, such as taking detailed pictures of security measures and testing law enforcement response times. Had the OPM at (b)(3) 10 USC 130e (USACE)

Terrorist and criminal acts are often preceded by reconnaissance activities, such as taking detailed pictures of security measures and testing law enforcement response times.

Security Posture Guide,” further criminal actions by the intruder could have occurred if the intent of that intruder was to cause the destruction of dam operations. The Commanders and District Engineers, Portland and Seattle Districts, in coordination with the OPMs for (b)(3) 10 USC 130e (USACE)

(b)(3) 10 USC 130e (USACE) should prioritize resources to implement security requirements (see table 1) in accordance with USACE “Baseline Security Posture Guide.”

Significant Weaknesses Identified During Biannual Physical Security Inspections Were Not Always Corrected

(b)(3) 10 USC 130e (USACE)

(b)(3) 10 USC 130e (USACE)

Army

Regulation 190-13 requires physical security inspections of all MEVAs once every 2 years. A MEVA is a facility or area essential to accomplishing the installation or organization mission or an area vulnerable to a threat to destroy, damage, or tamper with property or equipment, including terrorism. Table 2 shows when personnel from the

⁶ The Portland District released a video of the intrusion on YouTube to request the community’s assistance in identifying the suspect through the Corps Watch Program. Based on the video, law enforcement apprehended the suspect and prosecuted him for trespassing.

Portland and Seattle Districts, Security and Law Enforcement Offices, completed their last inspection at each project, the number of security weaknesses found during the inspections, the number of security weaknesses that increase the risk of unauthorized access, and the number of weaknesses that were corrected.

**Table 2: Security Weaknesses Reported and Corrected
During Most Recent Physical Security Inspections**

Project	Date of Inspection	Overall Weaknesses	Weaknesses Affecting Unauthorized Access	
			Total	Corrected
(b)(3) 10 USC 130e (USACE)	May 3, 2011	(b)(3) 10 USC 130e (USACE)		
	February 2, 2011			
	May 5, 2010			
	April 19, 2010			
	March 1, 2011			

(FOUO) (b)(3) 10 USC 130e (USACE)

Personnel from the Portland and Seattle Districts, Security and Law Enforcement Offices, stated that OPMs were responsible for responding to the physical security inspection results and identifying corrective actions taken or planned to address the weaknesses. Army Regulation 190-13 requires actions taken in response to physical security inspections to be documented and provided to the installation commanders; in this case, the District Commanders. This requirement can be accomplished through the completion of a plan of actions and milestones addressing the steps required to mitigate the security weaknesses. However, personnel provided written responses to the physical security inspections for only (b)(3) 10 USC 130e (USACE). Their responses showed funding shortfalls were an impediment to correcting physical security weaknesses.

Army Regulation 190-13 also instructs commanders with insufficient resources to correct the weaknesses by informing a higher level of command about the resource constraints. Officials in the Portland and Seattle District, Offices of Security and Law Enforcement, submitted a Schedule 75, "Management Decision Package for Anti-Terrorism, Law Enforcement, Corrections, and Physical Security," to the Northwestern Division to obtain funding to meet these physical security shortfalls. Those requests were subsequently sent

to the Headquarters, USACE, Provost Marshall Office, which was responsible for requesting additional funding from the Department of the Army to meet physical security shortfalls. However, funding was not provided through this process, because civil works projects are funded under a separate appropriation (civil works operation and maintenance).

(FOUO) (b)(3) 10 USC 130e (USACE)

(b)(3) 10 USC 130e (USACE)

(b)(3) 10 USC 130e (USACE)

(b)(3) 10 USC 130e (USACE)

(FOUO) (b)(3) 10 USC 130e (USACE)

(b)(3) 10 USC 130e (USACE)

Physical Security Shortfalls Were Not Always Identified and Prioritized During USACE Budget Process

The Commanders and District Engineers, Portland and Seattle District, and the OPMs did not always implement the 11 Baseline Security Guide requirements, or correct physical security weaknesses identified during physical security inspections because they did not always identify security shortfalls or recognize the criticality them within the constraints of the USACE budget process.

7 (FOUO) (b)(3) 10 USC 130e (USACE)

~~(FOUO)~~ Specifically, the OPMs for (b)(3) 10 USC 130e (USACE) did not include physical security needs in the USACE FY 2011 or FY 2012 annual budget requests (civil works operation and maintenance). The OPM for (b)(3) 10 USC 130e (USACE) and (b)(3) 10 USC 130e (USACE) identified physical security needs (b)(3) 10 USC 130e (USACE)

(b)(3) 10 USC 130e (USACE) in his FY 2011 and FY 2012 annual budget requests. However, the Portland District and Northwestern Division did not identify those security needs as a high priority when each level of command re-prioritized funding needs. Instead, security needs were combined into one operation and maintenance budget submission based on the business line the needs supported. The USACE budget process grouped equipment repairs, safety needs, and security needs together within one operation and maintenance budget request for each USACE Business Line. (b)(3) 10 USC 130e (USACE)

However, those needs were not always a high priority or funded by USACE. The Commanders and District Engineers, Portland and Seattle Districts, in coordination with the OPMs, should make physical security needs a higher priority to increase the likelihood those needs are funded under the existing USACE budgeting process, and develop plans of action and milestones to mitigate the weaknesses reported during the physical security inspections.

~~(FOUO)~~ By not effectively implementing all 11 requirements designed to detect and protect against unauthorized access or correcting physical security weaknesses, the Commanders and District Engineers, Portland and Seattle Districts, and OPMs increased the risk that significant loss of life and economic damages to USACE and local communities could occur if the structures were destroyed. Table 3 summarizes the greatest (worst-case scenario) potential loss of life and economic impact for each project, if compromised, based on USACE consequence assessment reports.

~~(FOUO)~~ Table 3: Potential Loss of Life and Economic Impact of Dam Compromise

Project	Loss of Life	Economic Impact (in millions)		
		To Rebuild Structure	To Local Community	Total
(b)(3) 10 USC 130e (USACE)	(b)(3) 10 USC 130e (USACE)			
Total				

Conclusion

USACE owns and operates 702 Civil Works structures that generate power, support navigation, protect communities from floods, provide recreational activities, and support the environment. Although all USACE Civil Works structures are not critical infrastructure, the USACE Office of Homeland Security designated all five projects reviewed as critical infrastructure. The National Infrastructure Protection Plan requires critical infrastructure to be protected from physical and cyber attacks because these types of attacks could disrupt Government and business services and result in significant loss of human life or economic damages.

~~(FOUO)~~ The five projects primarily produce hydropower or protect local communities from devastating floods. Therefore, protection and detection measures are critical to limiting the potential of unauthorized access to critical infrastructure and physical attacks.

(b)(3) 10 USC 130e (USACE)

Management Comments on the Finding and Our Response

Summaries of management comments on the finding and our response are in Appendix C.

Recommendations, Management Comments, and Our Response

Revised and Deleted Recommendations

As a result of management comments, we revised draft Recommendations A.1.a, A.1.c, A.6.a.(1) and A.6.a.(3) to more clearly meet the

(b)(3) 10 USC 130e (USACE)

In addition, we revised draft Recommendations A.3 and A.6.b to clarify the intent of testing physical access and law enforcement and project personnel responses to security incidents. We request that the Commander and District Engineer, Portland District, provide comments on the final report by February 13, 2013. We also deleted draft Recommendations A.6.a.(4)

(b)(3) 10 USC 130e (USACE)

(b)(3) 10 USC 130e (USACE)

A.1. We recommend that the Commander and District Engineer, Portland District, in coordination with the Operations Project Manager for , implement physical security measures in accordance with the Headquarters, U.S. Army Corps of Engineers memorandum, "Baseline Security Posture Guide for Civil Works Projects," December 10, 2004, as follows:

(FOUO) a. (b)(3) 10 USC 130e (USACE)

(FOUO) b. (b)(3) 10 USC 130e (USACE)

(FOUO) c. (b)(3) 10 USC 130e (USACE)

(FOUO) d. (b)(3) 10 USC 130e (USACE)

USACE Comments

(FOUO) The Chief, Operations Division, USACE, Civil Works, responding on behalf of the Commander and District Engineer, Portland District, agreed, stating that the implementation of (b)(3) 10 USC 130e (USACE)

In addition, he stated that adjustments for communications would be made where bandwidth for remote sites was available, but also stated that a risk and cost-benefit analysis was needed to determine whether manning or installing communications infrastructure was more practical. However, he also pointed out that the recommendations related (b)(3) 10 USC 130e (USACE)

either exceeded or did not meet the intent of the Baseline Security Posture Guide.

Our Response

Comments from the Chief, Operations Division, were responsive to the intent of the recommendations. Based on management comments and further review of the requirements, we revised two recommendations to ensure required actions fully aligned with Baseline Security Posture requirements. However, the comments did not include a completion date for implementing physical security upgrades at (b)(3) 10 USC 130e (USACE). Therefore, we request that the Commander and District Engineer, Portland District, provide the completion date for the planned actions.

A.2. We recommend that the Commander and District Engineer, Portland District, in coordination with the Operations Project Managers for (b)(3) 10 USC 130e (USACE),
(b)(3) 10 USC 130e (USACE) :

a. Prioritize physical security needs within the confines of the existing USACE budget process, to increase the likelihood those needs are funded.

USACE Comments

~~(FOUO)~~ The Chief, Operations Division, agreed, stating that priorities for meeting physical security requirements would be reviewed. However, he stated that the implication that the Portland District did not prioritize physical security funding was false and pointed out that funding for USACE projects was a complex and intricate process that could not be “captured in the broad brush of this audit report.” He also stated that the Portland District and OPMs would continue to prioritize physical security needs, make budget decisions when available resources did not meet available funding, and notify the next higher echelon about budget shortfalls. Further, he cited an agreement between USACE and the Bonneville Power Administration that provides security funding through a dedicated line-item for Portland District hydropower projects.

Our Response

~~(FOUO)~~ Comments from the Chief, Operations Division, were partially responsive. We understand that hydropower projects in the Portland District received funding from the Bonneville Power Administration for security to support the hydropower mission, but that funding was based on the percentage of the project that supported hydropower purposes. We also commend USACE for recognizing the importance of prioritizing physical security funding and reporting shortfalls to the next higher level of command; however, that process did not always occur. ~~(b)(3) 10 USC 130e (USACE)~~

~~(b)(3) 10 USC 130e (USACE)~~

~~(FOUO)~~ Further, solutions to mitigate physical security weaknesses found during physical security inspections were not always included in the projects’ budget submissions. Specifically, the physical inspections showed ~~(b)(3) 10 USC 130e (USACE)~~

~~(b)(3) 10 USC 130e (USACE)~~

Therefore, we request that the Commander and District Engineer, Portland District, reconsider his position about prioritizing security needs and provide comments on the final report by February 13, 2013.

b. Prioritize the results of physical security inspections and develop plans of action and milestones to mitigate weaknesses that, if left unaddressed, could unnecessarily increase the risk of compromise resulting from unauthorized access to the structure.

USACE Comments

~~(FOUO)~~ The Chief, Operations Division, agreed, stating that a plan of action was essentially developed as a result of physical security inspections, but acknowledged a more detailed plan could be developed as a part of the project's audit reports.

Our Response

Comments from the Chief, Operations Division, were responsive; however, the comments did not include a completion date for requiring the use of more detailed plan of action and milestones. Therefore, we request that the Commander and District Engineer, Portland District, provide the completion date for initiating the planned actions.

~~(FOUO)~~ A.3. (b)(3) 10 USC 130e (USACE)



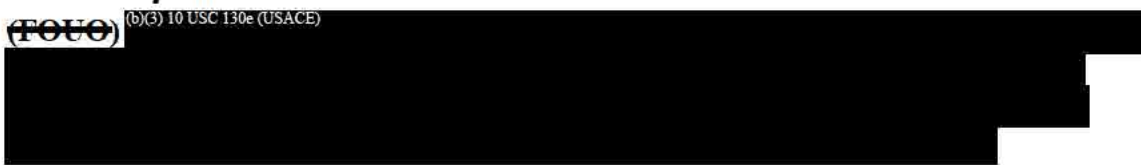
USACE Comments

~~(FOUO)~~ (b)(3) 10 USC 130e (USACE)



Our Response

~~(FOUO)~~ (b)(3) 10 USC 130e (USACE)



(FOUO)

(b)(3) 10 USC 130e (USACE)

(b)(3) 10 USC 130e (USACE)

(FOUO) Also, we did not misunderstand the DoDI 8500.2 requirements; DoDI 8500.2 control ECMT-2 pertains to conducting system penetration testing and control PEPS-1 pertains to conducting physical penetration testing of facilities. DoDI 8500.2 control PEPS-1 not only relates to facilities that process classified information (Attachment 4 to Enclosure 4, "Confidentiality Controls for DoD Information Systems Processing Classified Information"), but also those that process sensitive information (Attachment 4, Enclosure 5, "Confidentiality Controls for DoD Information Systems Processing Sensitive Information").

(b)(3) 10 USC 130e (USACE)

A.4. We recommend that the Commander and District Engineer, Seattle District, in coordination with the Operations Project Manager for [REDACTED], implement physical security measures in accordance with the Headquarters, U.S. Army Corps of Engineers memorandum, "Baseline Security Posture Guide for Civil Works Projects," December 10, 2004, by:


(FOUO) a.

(b)(3) 10 USC 130e (USACE)

USACE Comments

~~(FOUO)~~

(b)(3) 10 USC 130e (USACE)



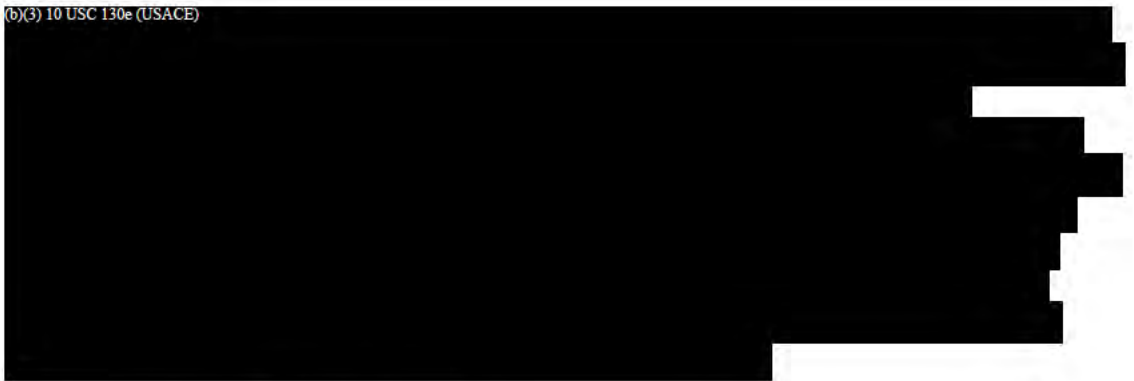
Our Response

~~(FOUO)~~ Comments from the Chief, Operations Division, were partially responsive.

(b)(3)
10
USC




(b)(3) 10 USC 130e (USACE)



~~(FOUO)~~ b.

(b)(3) 10 USC 130e (USACE)



~~(FOUO)~~ (b)(3) 10 USC 130e (USACE)

USACE Comments

~~(FOUO)~~ (b)(3) 10 USC 130e (USACE)

Our Response

Comments from the Chief, Operations Division, were responsive; therefore, no further comments were required.

A.5. We recommend that the Commander and District Engineer, Seattle District, in coordination with the Operations Project Managers for (b)(3) 10 USC 130e (USACE) and (b)(3) 10 USC 130e (USACE) :

a. Prioritize physical security needs within the confines of the existing USACE budget process, to increase the likelihood those needs are funded.

USACE Comments

~~(FOUO)~~ The Chief, Operations Division, agreed, stating that the need to prioritize physical security occurred throughout the budget process. However, he stated that the implication that the Seattle District did not prioritize physical security funding was false and pointed out that funding for USACE projects was a complex and intricate process that could not be “captured in the broad brush of this audit report.” He also stated that the Seattle District and OPMs would continue to prioritize physical security needs, make budget decisions when available resources did not meet available funding, and notify the next higher echelon about budget shortfalls. In addition, the Chief, Operations Division, cited an agreement between USACE and the Bonneville Power Administration that provides security funding through a dedicated line-item for (b)(3) 10 USC 130e (USACE) that has provided approximately \$750,000 in funding for security since the terrorist attacks of September 11, 2001; he also stated that (b)(3) 10 USC 130e (USACE) identifies nonroutine security needs and requests funding for those needs through the Bonneville Power Administration Small Capital Expenditure Program. Further, he stated that (b)(3) 10 USC 130e (USACE) was using its operation and maintenance funds for security upgrades in FY 2013.

Our Response

Comments from the Chief, Operations Division, were partially responsive. We commend USACE for recognizing the importance of prioritizing physical security funding and reporting shortfalls to the next higher level of command, but documentation showed that process did not always occur. We understand that (b)(3) 10 USC 130e (USACE) submits separate funding requests to the Bonneville Power Administration to meet North American Electric Reliability Corporation Critical Infrastructure Protection requirements. We also understand that the requests, particularly those related to securing critical assets related to the hydropower mission, are generally funded. In addition to submitting budget requests

to the Bonneville Power Administration, we understand that (b)(3) 10 USC 130e (USACE) submits budget requests to obtain USACE appropriations. However, documentation supporting USACE budget submissions from the Seattle District for (b)(3) 10 USC 130e (USACE) FY 2011 and FY 2012 did not itemize specific shortfalls or needs associated with the requested funding. For example, the (b)(3) 10 USC 130e (USACE) budget request showed annual operating activity costs or general maintenance and repair costs and the (b)(3) 10 USC 130e (USACE) budget request showed a summary line total for power generation and joint capital costs.

Without documentation showing individual security needs and how they were prioritized for these two projects in FY 2011 and FY 2012, the Seattle District was unable to support whether the security shortfalls found during physical security inspections or those found during the audit were included in those requests. Therefore, we request that the Commander and District Engineer, Seattle District, reconsider his position about how security needs are prioritized and provide comments on the final report by February 13, 2013.

b. Prioritize the results of physical security inspections and develop plans of action and milestones to mitigate weaknesses that, if left unaddressed, could unnecessarily increase the risk of compromise resulting from unauthorized access to the structure.

USACE Comments

~~(FOUO)~~ The Chief, Operations Division, agreed, stating that the Seattle District and OPMs would be more conscientious in prioritizing, addressing, and tracking the remediation of findings from annual physical security inspections through the use of a maintenance management system. He also stated that the Seattle District prioritizes necessary expenditures at its projects based on appropriations that it receives, and he noted that prioritizing security against operational needs could jeopardize the critical infrastructure that the security measures are intended to protect.

Our Response

Comments from the Chief, Operations Division, were responsive; however, they did not include a completion date for prioritizing, addressing, and tracking the remediation of findings that resulted from physical security inspections. Therefore, we request that the Commander and District Engineer, Seattle District, provide the completion date for the planned actions.

A.6. We recommend that the Commander and District Engineer, Seattle District, in coordination with the Operations Project Manager for (b)(3) 10 USC 130e (USACE) dam:

a. Implement physical security measures in accordance with the Headquarters, U.S. Army Corps of Engineers memorandum, "Baseline Security Posture Guide for Civil Works Projects," December 10, 2004, as follows:

(FOUO) 1. (b)(3) 10 USC 130e (USACE)

(FOUO) 2. (b)(3) 10 USC 130e (USACE)

(FOUO) 3. (b)(3) 10 USC 130e (USACE)

USACE Comments

(FOUO) The Chief, Operations Division, agreed, stating that the OPM for (b)(3) 10 USC 130e programmed \$40,000 to fund an October 2012 security assessment that the Corps of Engineers Huntsville Design Center of Expertise was to perform to identify required security upgrades needed to meet Baseline Security Posture Guide requirements. He also stated that funds would be programmed from annual appropriations to implement recommendations to improve security.

Our Response

Comments from the Chief, Operations Division, were responsive; however, they did not include a completion date implementing required security upgrades once the assessment is completed. Therefore, we request that the Commander and District Engineer, Seattle District, provide the completion date for the planned actions.


(FOUO) b. (b)(3) 10 USC 130e (USACE)

USACE Comments


(FOUO) The Chief, Operations Division, disagreed, stating we misunderstood DoDI 8500.2 IA controls. Specifically, he stated that DoDI 8500.2 control ECMT-2 pertains to conducting periodic, unannounced attempts to obtain virtual (logical) access to a system, but also agreed DoDI 8500.2 control PEPS-1 requires facility penetration testing of key computing facilities. However, he stated that DoDI 8500.2 control PEPS-1 pertained to systems processing classified information (Attachment 4 to Enclosure 4, "Confidentiality Controls for DoD Information Systems Processing Classified Information"). In addition, he stated that Army Regulation 190-13 prohibits physical security inspectors from engaging in illegal or dangerous conduct to demonstrate security weaknesses. Further, he stated that misapplying a standard for classified networks and conducting physical security testing that includes attempts to forcibly gain access to the project was not appropriate, safe, or prudent based on the Seattle District's understanding of the requirements.

Our Response

~~(FOUO)~~ Comments from the Chief, Operations Division, were partially responsive. The intent of our recommendation was not for physical security specialists to engage in illegal or unsafe practices. Rather, our intent was for the project OPM and Security and Law Enforcement Office, Seattle District, to conduct periodic exercises, in coordination with project personnel and local law enforcement, to test overall security measures and responses to threat scenarios that simulate realistic and potential security incidents that could occur at ~~(b)(3) 10 USC 130e (USACE)~~. This type of testing was already completed at another USACE project. ~~(b)(3) 10 USC 130e (USACE)~~



~~(FOUO)~~ ~~(b)(3) 10 USC 130e (USACE)~~



Finding B. Systems Used to Operate Critical Infrastructure in the Northwestern Division Were Not Always Protected Against Cyber Threats

The OPMs for the five projects designated as critical infrastructure by the USACE Office of Homeland Security did not effectively and consistently secure and protect the Willamette Valley (b)(3) 10 USC 130e (USACE) from

internal and external cyber threats. Specifically, the OPMs for (b)(3) 10 USC 130e (USACE) and the (b)(3) 10 USC 130e (USACE) for (b)(3) 10 USC 130e (USACE) did not always effectively implement (b)(3) 10 USC 130e (USACE)

- (b)(3) 10 USC 130e (USACE)

- (b)(3) 10 USC 130e (USACE)

- (FOUO) (b)(3) 10 USC 130e (USACE)

- (FOUO) (b)(3) 10 USC 130e (USACE)

Also, the Commanders and District Engineers, Portland and Seattle Districts, and the GDACS IA manager did not appoint, in writing, all personnel performing key IA responsibilities for the ICSs used to operate (b)(3) 10 USC 130e (USACE)

Personnel were not always appointed in accordance with DoDI 8500.2 requirements because Commanders and the GDACS IA manager did not know those positions were required to be appointed in writing.

(FOUO) In addition, the OPMs for the five projects did not effectively implement (b)(3) 10 USC 130e (USACE)

(FOUO) (b)(3) 10 USC 130e (USACE)

ICS Security Configurations and Known Vulnerabilities Were Not Adequately Managed

(FOUO)

(b)(3) 10 USC 130e (USACE)

(b)(3) 10 USC 130e (USACE)

(FOUO) Table 4. System Security and Vulnerability Management Weaknesses

(b)(3) 10 USC 130e (USACE)

(FOUO)

(b)(3) 10 USC 130e (USACE)

(FOUO)

(b)(3) 10 USC 130e (USACE)

Willamette Valley SCADA System Was Not Adequately Protected

(FOUO) (b)(3) 10 USC 130e (USACE)
[Redacted]

(FOUO) System Security Requirements Were Not Configured or Effective

(FOUO) (b)(3) 10 USC 130e (USACE)
[Redacted]


(FOUO) (b)(3) 10 USC 130e (USACE)
[Redacted]

A small rectangular box containing a heavily redacted image, possibly a logo or diagram, with a double border.

[Redacted]

⁸ (FOUO) (b)(3) 10 USC 130e (USACE)
[Redacted]


(FOUO) (b)(3) 10 USC 130e (USACE)



(FOUO) (b)(3) 10 USC 130e (USACE)



The OPM and system administrators stated that they did not begin considering (b)(3) 10 USC 130e (USACE)




(FOUO) The Portland District Chief of Operations and the Willamette Valley Project OPM began actions to certify and accredit the Willamette Valley (b)(3) 10 USC 130e (USACE) in June 2010. (b)(3) 10 USC 130e (USACE)


(FOUO) (b)(3) 10 USC 130e (USACE)



(b)(3) 10 USC 130e (USACE)



(b)(3) 10 USC 130e (USACE)



⁹ Until 2009, all information systems within the Portland and Seattle District, including ICSs used to operate water control structures, were included in (b)(3) 10 USC 130e (USACE) for each District.

~~(FOUO)~~ Vulnerabilities Were Neither Identified Nor Mitigated

~~(FOUO)~~

(b)(3) 10 USC 130e (USACE)

[REDACTED]

(b)(3) 10 USC 130e (USACE)

~~(FOUO)~~

(b)(3) 10 USC 130e (USACE)

[REDACTED]

~~(FOUO)~~

(b)(3) 10 USC 130e (USACE)

[REDACTED]

¹⁰ An IAVA is a comprehensive process that notifies DoD personnel about vulnerabilities affecting their information systems and networks; they include implementation strategies to reduce the risk associated with identified vulnerabilities. An IAVA is generated whenever a critical vulnerability that poses an immediate threat to DoD exists.

(FOUO)

(b)(3) 10 USC 130e (USACE)

Management Took Actions to Mitigate Risks Affecting the Willamette Valley SCADA System

Although the Willamette Valley Project was expected to begin

(b)(3) 10 USC 130e (USACE)

- (FOUO)

(b)(3) 10 USC 130e (USACE)

- (FOUO)

(b)(3) 10 USC 130e (USACE)

- (FOUO)

(b)(3) 10 USC 130e (USACE)

- (FOUO)

(b)(3) 10 USC 130e (USACE)

- (FOUO)

(b)(3) 10 USC 130e (USACE)

- (FOUO)

(b)(3) 10 USC 130e (USACE)

- (FOUO)

(b)(3) 10 USC 130e (USACE)

(FOUO)

(b)(3) 10 USC 130e (USACE)

(FOUO)

(b)(3) 10 USC 130e (USACE)

¹¹ The Willamette Valley Project and Portland District reprioritized operational needs to fund between \$50,000 and \$70,000 in costs to mitigate the risks that they considered more significant to operations.

(FOUO)

(b)(3) 10 USC 130e (USACE)

(FOUO)

(b)(3) 10 USC 130e (USACE)

Although the USACE goal of consolidating operation and maintenance funding by business line is to provide greater flexibility in managing budgets, cyber security risk mitigation and weaknesses are not always considered when funding is authorized. The Headquarters, USACE, Programs Division, should revise the current USACE budget process to ensure IA requirements are adequately funded.

GDACS Was Not Adequately Protected

(FOUO)

(b)(3) 10 USC 130e (USACE)

(FOUO)

(b)(3) 10 USC 130e (USACE)

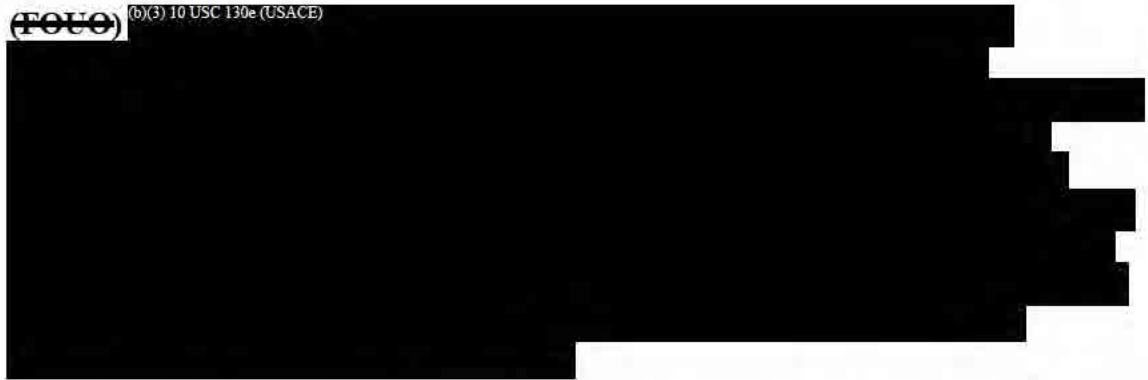
(FOUO)

(b)(3) 10 USC 130e (USACE)

(b)(3) 10 USC 130e (USACE)








(FOUO) (b)(3) 10 USC 130e (USACE)




(FOUO) More Frequent Vulnerability Assessments Were Needed

(FOUO) The GDACS Maintenance Team conducted annual vulnerability assessments of GDACS servers at each hydropower project in the Northwestern Division, including (b)(3) 10 USC 130e (USACE) however, the frequency of the assessments were not sufficient to promptly identify and mitigate known vulnerabilities that could disrupt power generation to the Pacific Northwest. (b)(3) 10 USC 130e (USACE)




- (FOUO) (b)(3) 10 USC 130e (USACE) 
- (FOUO) (b)(3) 10 USC 130e (USACE) 
- (FOUO) (b)(3) 10 USC 130e (USACE) 
- (FOUO) (b)(3) 10 USC 130e (USACE) 

(FOUO) (b)(3) 10 USC 130e (USACE)




(FOUO)

(b)(3) 10 USC 130e (USACE)




(FOUO)

(b)(3) 10 USC 130e (USACE)




(FOUO)

(b)(3) 10 USC 130e (USACE)



(FOUO)

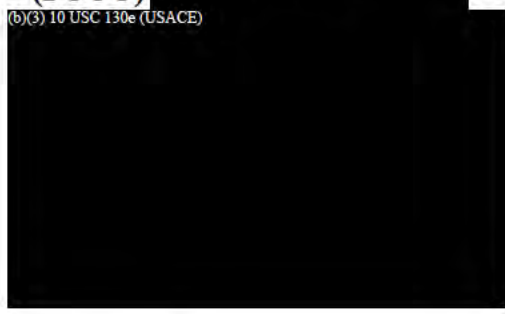
(b)(3) 10 USC 130e (USACE)




(FOUO)

(b)(3) 10 USC 130e (USACE)


(b)(3) 10 USC 130e (USACE)




(b)(3) 10 USC 130e (USACE)



(b)(3) 10 USC 130e (USACE)



12 (b)(3) 10 USC 130e (USACE)



(FOUO) We do not consider conducting annual vulnerability assessments to be sufficient for adequately protecting information systems, especially those used to operate critical infrastructure that generates hydropower and provides flood control, from emerging threats and known vulnerabilities. ICSs have become more frequent targets of cyber attacks and new vulnerabilities, which could degrade the security posture of these systems, are constantly emerging. To effectively protect these systems from those vulnerabilities, the GDACS Maintenance Team must promptly identify the vulnerabilities to ensure appropriate actions, such as installing recommended security patches, can be taken to mitigate the risks. The GDACS Maintenance Team should conduct more frequent vulnerability assessments on GDACS servers at all projects, including (b)(3) 10 USC 130e (USACE) [REDACTED], to promptly identify and mitigate known vulnerabilities that could allow specifically designed cyber attacks to exploit known vulnerabilities affecting a (b)(3) 10 USC 130e (USACE) [REDACTED].

(FOUO) (b)(3) 10 USC 130e (USACE) [REDACTED]

(FOUO) (b)(3) 10 USC 130e (USACE) [REDACTED]

~~(FOUO)~~

(b)(3) 10 USC 130e (USACE)

~~(FOUO)~~

(b)(3) 10 USC 130e (USACE)

~~(FOUO)~~

(b)(3) 10 USC 130e (USACE)

~~(FOUO)~~

(b)(3) 10 USC 130e (USACE)

System Security Configuration Requirements Were Not Implemented or Effective

~~(FOUO)~~

(b)(3) 10 USC 130e (USACE)

~~(FOUO)~~

(b)(3) 10 USC 130e (USACE)

(FOUO)

(b)(3) 10 USC 130e (USACE)

(b)(3) 10 USC 130e (USACE)

(FOUO)

(b)(3) 10 USC 130e (USACE)

(FOUO)

(b)(3) 10 USC 130e (USACE)

(FOUO)

(b)(3) 10 USC 130e (USACE)

(FOUO)

(b)(3) 10 USC 130e (USACE)



(FOUO)

(b)(3) 10 USC 130e (USACE)

IA Appointments Were Generally Not in Writing and Personnel Performing IA Responsibilities Did Not Always Have Experience

The IA manager for (b)(3) 10 USC 130e (USACE) did not appoint, in writing, the system administrators at (b)(3) 10 USC 130e (USACE). In addition, the Commanders and District Engineers, Portland and Seattle Districts, did not appoint, in writing, an IA manager or the system administrators performing IA responsibilities for (b)(3) 10 USC 130e (USACE).¹⁴ DoDI 8500.2 control DCSD-1 (IA Documentation) requires all IA appointments to be established in writing and include assigned duties and appointment criteria, such as training, security clearance, and information technology designation. IA managers are responsible for the overall IA program for an information system, and system administrators maintain, configure, and administer access to information systems.

The OPMs for (b)(3) 10 USC 130e (USACE) that used (b)(3) 10 USC 130e (USACE) stated that the Commanders and District Engineers, Portland and Seattle Districts, did not appoint, in writing, IA managers because they were either unaware of this requirement or thought those positions were only required for certified and accredited systems. In addition, the OPMs for (b)(3) 10 USC 130e (USACE) did not appoint, in writing, system administrators for the (b)(3) 10 USC 130e (USACE) because they did not know those positions were required to be appointed in writing.

Although the GDACS IA Security Officer stated that system administrators were appointed for (b)(3) 10 USC 130e (USACE), he could not provide documentation to support those appointments. The lack of documentation led us to conclude that these appointments were not made in writing as required by DoD 8570.01-M, "Information Assurance Workforce Improvement Program," January 24, 2012. Specifically, DoD 8570.01-M, requires all personnel in technical and management roles performing IA responsibilities to be appointed in writing to ensure that personnel clearly understand their assigned roles and responsibilities. After we brought this issue to the attention of the GDACS IA manager, the Commander and District Engineer, Portland District, issued an appointment letter, effective July 19, 2012, for the three system administrators at (b)(3) 10 USC 130e (USACE). Because the Commander and District Engineer, Portland District, issued a formal appointment to the three (b)(3) 10 USC 130e (USACE), we did not make recommendations to appoint, in writing, those personnel.

~~(FOUO)~~ In addition, the OPM for (b)(3) 10 USC 130e (USACE) allowed the system administrator access to the (b)(3) 10 USC 130e (USACE) without ensuring that that person had

¹⁴ ~~(FOUO)~~ (b)(3) 10 USC 130e (USACE)

~~(FOUO)~~ adequate experience and training in accordance with DoD 8570.01-M. DoD 8570.01-M requires all personnel performing IA responsibilities to be certified and meet agency training requirements. In addition, Army Regulation 25-2, requires system administrators to obtain, at a minimum, an IA technical level I certification and identifies training requirements needed to meet this certification level.

~~(FOUO)~~ (b)(3) 10 USC 130e (USACE)
[REDACTED]

~~(FOUO)~~ (b)(3) 10 USC 130e (USACE)
[REDACTED] Actions by the untrained person could not only adversely affect the information system, but also disrupt project operations. The Commanders and District Engineers, Portland and Seattle Districts, must ensure that all personnel performing IA responsibilities are not only appointed in writing, but are also technically capable of performing those roles and responsibilities in accordance with DoD 8570.01-M requirements.

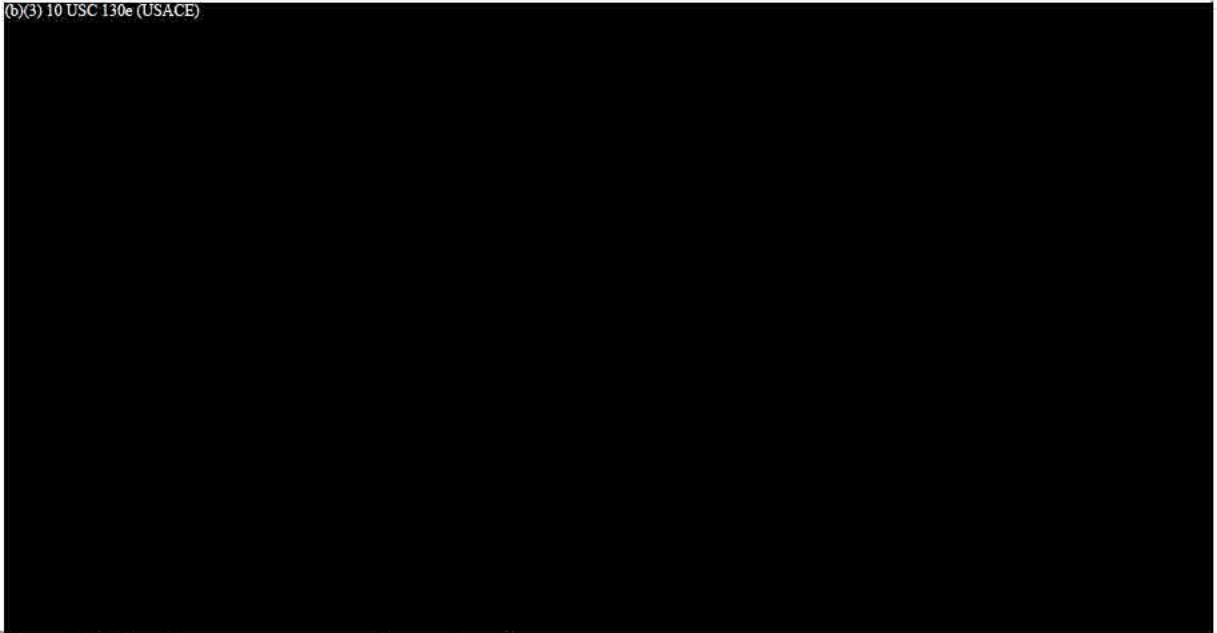
Access to the ICSs Used to Operate Critical Infrastructure Was Not Effectively Managed

~~(FOUO)~~ The OPMs for the five projects did not effectively implement procedures, and
(b)(3) 10 USC 130e (USACE)
[REDACTED]

¹⁵ Automated Control Systems Incorporated turned over operation of the PLC-based information system to (b)(3) 10 USC 130e (USACE), but continued to provide maintenance services as needed.

~~(FOUO)~~ Table 5. IA Weaknesses That Limit the Effectiveness of Controlling Access to Authorized Personnel Only

(b)(3) 10 USC 130e (USACE)

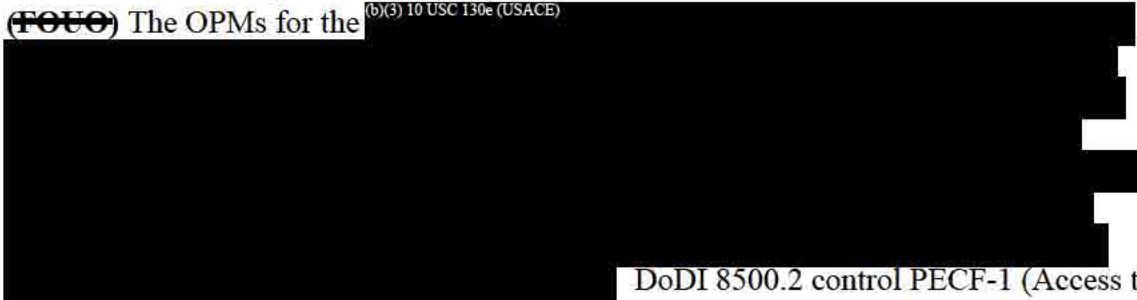


Note: Blank cells represent no weakness found.

~~(FOUO)~~ ***Physical Access to the Control Rooms Housing the ICSs Was Not Strictly Controlled***

~~(FOUO)~~ The OPMs for the

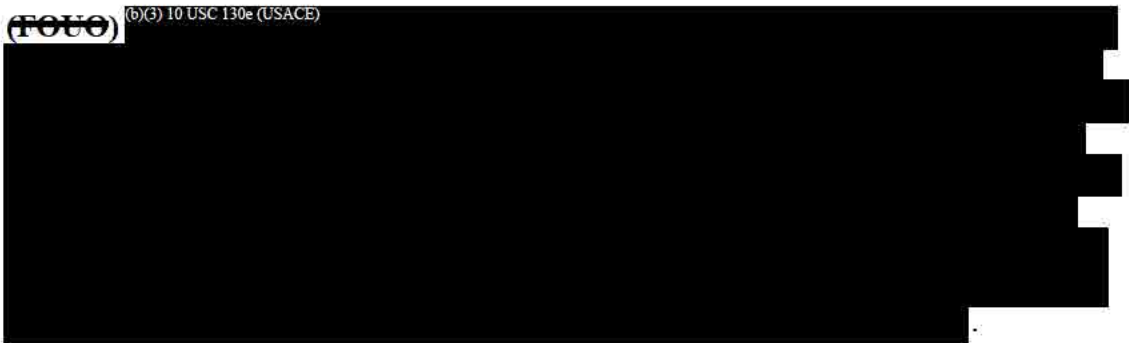
(b)(3) 10 USC 130e (USACE)




DoDI 8500.2 control PECF-1 (Access to Computing Facilities) requires only authorized personnel with a need-to-know to be granted physical access to computing facilities. Also, DoDI 8500.2 control PEPF-1 (Physical Protection of Facilities) requires every physical access point to facilities housing workstations that process or display sensitive information or unclassified information that has not been cleared for release to be controlled.

~~(FOUO)~~

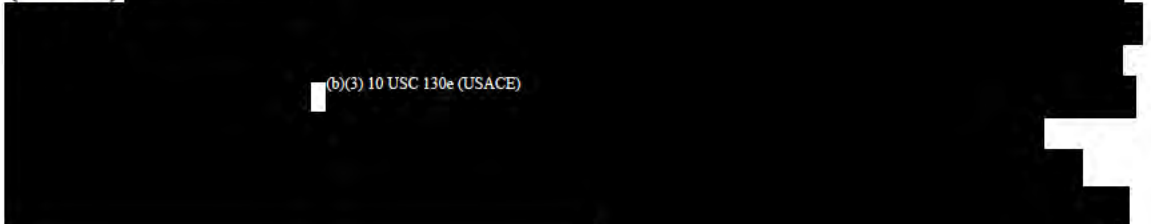
(b)(3) 10 USC 130e (USACE)



(FOUO) Consequently, the OPMs for (b)(3) 10 USC 130e (USACE)




(FOUO) (b)(3) 10 USC 130e (USACE)



(b)(3) 10 USC 130e (USACE)



(FOUO) (b)(3) 10 USC 130e (USACE)



¹⁶ (FOUO) The Designated Accrediting Authority granted an operational exemption allowing GDACS to use shared or group accounts to support operations during the certification and accreditation process based on Portland District-developed documentation, "GDACS System IA Control Exceptions," February 2009.

Documentation Did Not Support an Approved Operational Need for Access to the ICSs

The OPMs for the five projects (b)(3) 10 USC 130e (USACE)

DoDI 8500.2 control IAAC-1 (Account Control) requires system owners to implement a comprehensive account management process to ensure that only authorized users can access DoD information systems. Although DoDI 8500.2 control IAAC-1 does not specifically require written documentation to support access authorizations, NIST SP 800-53, "Recommended Security Controls for Federal Information Systems and Organizations," May 1, 2010, requires access to be granted based on valid access authorizations.¹⁷ Table 6 identifies the number of personnel with logical access to the ICSs without a documented and formally approved access request form.

Table 6: Number of Personnel at Each Project With Logical Access to the ICSs

Project	System Administrators	Operators	Chief Operators
(b)(3) 10 USC 130e (USACE)			
* (b)(3) 10 USC 130e (USACE)			

(b)(3) 10 USC 130e (USACE)

During 2011, the OPMs and reliability compliance coordinators for (b)(3) 10 USC 130e (USACE) implemented a process that now requires personnel

¹⁷ NIST SP 800-53 control AC-2 requires written access authorization requests.

requesting logical access to (b)(3) 10 USC 130e (USACE) to complete a written authorization request form.¹⁸
(b)(3) 10 USC 130e (USACE)

(b)(3) 10 USC 130e (USACE)

(b)(3) 10 USC 130e (USACE)

(b)(3) 10 USC 130e (USACE)

DoDI 8500.2

control PRRB-1 (Security Rules of Behavior or Acceptable Use Policy) requires rules describing IA operations of the DoD information system and clearly defined IA responsibilities and expected behavior of all personnel that prescribe the consequences of inconsistent behavior or noncompliance as a condition of access. After we informed the OPMs for (b)(3) 10 USC 130e (USACE) about the lack of

¹⁸ The OPMs and reliability compliance coordinators for (b)(3) 10 USC 130e (USACE) implemented the process to comply with North American Electric Reliability Corporation Critical Infrastructure Protection standard-004, "Cyber Security – Personnel and Training," January 24, 2011.

documentation, they created an acceptable use policy that was subsequently signed by all personnel performing IA responsibilities. Because the OPMs created appropriate documentation and all personnel that performed IA responsibilities for (b)(3) 10 USC 130e (USACE) have since signed those agreements, we did not make recommendations to those OPMs to take further action. However, the OPMs for (b)(3) 10 USC 130e (USACE) should ensure that IA responsibilities, expected behavior, and consequences of noncompliance are documented and acknowledged as part of the written process for obtaining logical access to the ICSs.

Conclusion

(FOUO)

(b)(3) 10 USC 130e (USACE)

The National Infrastructure Protection Plan requires critical infrastructure to be protected from physical and cyber attacks because these types of attacks could disrupt Government and business services and result in significant loss of human life or economic damages. Therefore, protection and detection measures are critical to limiting the potential of unauthorized access to the ICSs used to operate Civil Works critical infrastructure because cyber attacks can originate from within or outside USACE. In addition, the OPMs for all five projects did not implement effective procedures and IA controls to identify, manage, and mitigate known vulnerabilities affecting the (b)(3) 10 USC 130e (USACE); properly configure information security settings to detect and protect the systems against cyber attacks; and limit access to the controls rooms where the ICSs resided.

(FOUO)

(b)(3) 10 USC 130e (USACE)

Management Comments on the Finding and Our Response

Summaries of management comments on the finding and our response are in Appendix C.

Recommendations, Management Comments, and Our Response

Revised Recommendations

As a result of management comments, we revised draft Recommendations B.1, B.2.a, and B.2.c to clarify the intent of the recommendations. We request that the Chief, Programs Integration Division, and the Chief, Hydrologic Design Center, provide comments on the final report by February 13, 2013.

B.1. We recommend that the Chief, Programs Integration Division, Headquarters, U.S. Army Corps of Engineers,, revise the current budget process to separately identify information assurance requirements to ensure sufficient funding is available to protect the industrial control systems used to operate critical infrastructure from cyber security risks.

USACE Comments

The Chief, Operations Division, USACE, Civil Works, responding on behalf of Headquarters, USACE, Programs Integration Division, agreed, stating that the USACE, Civil Works, budget process considered all district and division funding requirements submitted using a complex prioritization process that evaluated competing needs. He stated that separate consideration is given to Operations Hydropower Business Line budget through a special budget category to address electric reliability cyber security requirements, which are defined in Engineering Regulation 1130-2-551, “Hydropower Operations and Maintenance Policy Bulk Power System Reliability Compliance Program,” September 30, 2009, and Engineering Pamphlet 1130-2-551, “Hydropower Operations and Maintenance Policy Implementation of Bulk Power System Reliability Compliance Program,” September 30, 2009. Further, he stated that all the cyber security requirements needed to meet the North American Electric Reliability Corporation Critical Infrastructure Protection requirements were fully funded.

In addition, the Chief, Operations Division, stated that the USACE Office of Homeland Security completed assessments of the Northwestern Division projects (portfolio) to identify and prioritize critical projects as the first step in implementing the Critical Infrastructure Protection and Resilience Program risk management framework. The framework is defined in Chapter 23, “Physical Security of Dams,” of Engineering Regulation 1110-2-1156, “Engineering and Design Safety of Dams – Policy and Procedures,” October 28, 2011. He stated that this process was recently completed at the five projects included in the scope of the audit. He also stated that the Office of Homeland Security, Operations Division, and Operational Protection Division would work together with the Programs Integration Division and USACE Business Line managers to update budget guidance to ensure that physical security requirements at critical facilities were properly incorporated into the FY 2015 budget process.

Our Response

Comments from the Chief, Operations Division, were partially responsive. We commend USACE for taking action to update its guidance for developing budgets to ensure that physical security requirements are funded beginning with the FY 2015 budget cycle. However, the intent of this recommendation pertained to ensuring that cyber security (IA) requirements for ICSs were specifically defined in the USACE budget as a discrete line item within the operation and maintenance line item for each respective business line. Although the Chief, Operations Division, stated that IA requirements were submitted to the USACE Programs Integration Division for separate consideration through the Operations Hydropower Business Line based on Engineering Regulation 1130-2-551 and Engineering Pamphlet 1130-2-551, this process only pertained to identifying cyber security shortfalls for hydropower projects, which account for only 75 of the 702 USACE water structures.

The IA Program Manager stated that the USACE, Office of Corporate Information (Information Technology), budget included a separate IA budget line, but acknowledged that ICSs were not included in that line item. The process described by the Chief, Operations Division, did not account for cyber security requirements to fund all other ICSs that did not support the Hydropower Business Line. We understand that select USACE projects obtained funding to address physical and cyber security shortfalls through other funding sources, such as the Bonneville Power Administration, when the projects were designated bulk electric producing projects (b)(3) 10 USC 130e (USACE)) to comply with North American Electric Reliability Corporation Critical Infrastructure Protection requirements. However, the USACE budget process for projects using an ICS that were not bulk electric projects did not specifically account for IA funding needs to ensure that those projects could adequately manage cyber security risks. Budget documentation for the five projects for FY 2011 and FY 2012 did not include IA funding needs despite the need for funding to mitigate cyber security weaknesses. Therefore, we request that the Program Development Branch Chief, Headquarters, USACE, Programs Integration Division, reconsider his position about developing a discrete IA line item within the operation and maintenance budget line and provide comments on the final report by February 13, 2013.

B.2. We recommend the Chief, Hydroelectric Design Center, in coordination with the Generic Data Acquisition Control System Maintenance Team:

(FOUO) a. (b)(3) 10 USC 130e (USACE)

USACE Comments

(FOUO) (b)(3) 10 USC 130e (USACE)

(FOUO) (b)(3) 10 USC 130e (USACE)
[Redacted]

(FOUO) (b)(3) 10 USC 130e (USACE)
[Redacted]

Our Response

(FOUO) (b)(3) 10 USC 130e (USACE)
[Redacted]

(FOUO) b. Perform more frequent vulnerability assessment scans of generic data acquisition control system servers at all projects using the system, including those supporting operations at (b)(3) 10 USC 130e (USACE)

[Redacted]

USACE Comments

(FOUO) (b)(3) 10 USC 130e (USACE)
[Redacted]

(FOUO) (b)(3) 10 USC 130e (USACE)
[Redacted]

Our Response

Comments from the Chief, Operations Division, were responsive; therefore, no further comments were required.

(FOUO) c.

(b)(3) 10 USC 130e (USACE)

USACE Comments

(FOUO)

(b)(3) 10 USC 130e (USACE)

(FOUO)

(b)(3) 10 USC 130e (USACE)

Our Response

(FOUO) Comments from the Chief, Operations Division, were partially responsive to the intent of the recommendation.

(b)(3) 10 USC 130e (USACE)

(FOUO) (b)(3) 10 USC 130e (USACE)

(FOUO) (b)(3) 10 USC 130e (USACE)

B.3. We recommend that the Commander and District Engineer, Seattle District, in coordination with the Operations Project Manager for (b)(3) 10 USC 130e (USACE) :

(FOUO) a. (b)(3) 10 USC 130e (USACE)

(FOUO) (1) (b)(3) 10 USC 130e (USACE)

(FOUO) (2) (b)(3) 10 USC 130e (USACE)

(FOUO) (3) (b)(3) 10 USC 130e (USACE)

(FOUO) (4) (b)(3) 10 USC 130e (USACE)

system.

(FOUO) (5) (b)(3) 10 USC 130e (USACE)

b. Appoint, in writing, an information assurance manager and a qualified system administrator for the programmable logic controller-based information system in accordance with DoD Instruction 8500.2, "Information Assurance (IA)

Implementation,” February 6, 2003, and DoD 8570.01-M, “Information Assurance Workforce Improvement Program,” January 24, 2012, requirements.

(FOUO) c. (b)(3) 10 USC 130e (USACE)

d. Update existing standard operating procedures, “Logical Access Administration and Access Procedures,” March 29, 2012, to include documentation requirements for requesting and approving logical access to the programmable logic controller-based information system, and based on that process, ensure that all personnel authorized logical access have signed and approved documentation that demonstrates their justification and need-to-know.

e. Develop an acceptable use policy that defines information assurance responsibilities, expected behavior, and consequences of noncompliance with the policy, and require all personnel performing information assurance roles to sign the agreement as part of the written process for obtaining logical access to the programmable logic controller-based information system in accordance with DoD Instruction 8500.2, “Information Assurance (IA) Implementation,” February 6, 2003, requirements.

USACE Comments

(FOUO) (b)(3) 10 USC 130e (USACE)

Our Response

(FOUO) (b)(3) 10 USC 130e (USACE)

B.4. We recommend the Commander and District Engineer, Portland District, in coordination with the Operations Project Managers for (b)(3) 10 USC 130e (USACE) :

a. Appoint, in writing, an information assurance manager and system administrators for the Willamette Valley supervisory control and data acquisition system, and after transitioning to the generic data acquisition control system, appoint, in writing, personnel performing information assurance responsibilities in


accordance with DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003, and DoD 8570.01-M, "Information Assurance Workforce Improvement Program," January 24, 2012, requirements.

USACE Comments

~~(FOUO)~~ The Chief, Operations Division, agreed, stating that the Commander and District Engineer, Portland District, appointed, in writing, a qualified system administrator. The Chief, Operations Division, pointed out that the Portland District was moving forward with installing GDACS at Willamette Valley projects. In addition, he stated that future appointments and training for personnel performing IA responsibilities would occur as GDACS was installed throughout the Willamette Valley.

Our Response

~~(FOUO)~~ Comments from the Chief, Operations Division, were partially responsive to the intent of the recommendation. Although the Commander and District Engineer, Portland District, appointed, in writing, a qualified and trained system administrator, (b)(3) 10 USC 130e
(USACE)



b. Develop standard operating procedures for granting logical access to the Willamette Valley supervisory control and data acquisition system, including documentation requirements for requesting and approving logical access, and based on that process, ensure that all personnel authorized logical access have signed and approved documentation that demonstrates their justification and need-to-know.

USACE Comments

~~(FOUO)~~ The Chief, Operations Division, agreed, stating that the Willamette Valley would begin using existing procedures that the projects along the Columbia River (using GDACS) use to document access requirements and approved logical access. He stated that personnel with logical access to the Willamette Valley SCADA system would complete documentation requirements by December 2012.

Our Response

Comments from the Chief, Operations Division, were responsive; therefore, no further comments were required.

c. Develop an acceptable use policy that defines information assurance responsibilities, expected behavior, and consequences of noncompliance with the policy, and require all personnel performing information assurance roles to sign the agreement as part of the written process for obtaining logical access to the Willamette Valley supervisory control and data acquisition system in accordance with DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003, requirements.

USACE Comments

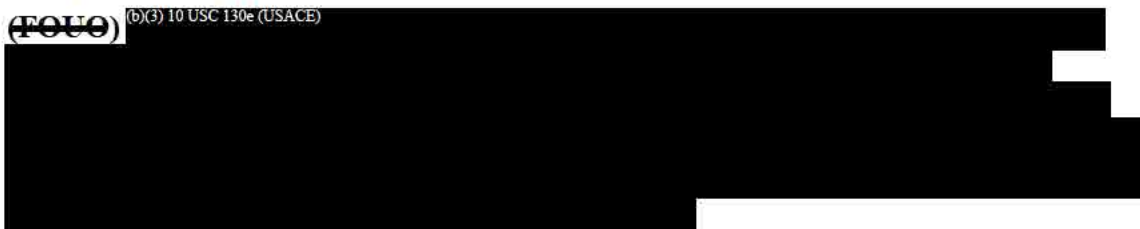
~~(FOUO)~~ The Chief, Operations Division, agreed, stating that the Willamette Valley would begin using the Acceptable Use Policy developed for GDACS because it was generic and could be adopted and reused by personnel with IA responsibilities for the Willamette Valley SCADA system. He pointed out that the system administrator for the Willamette Valley SCADA system already signed the agreement and that any personnel assigned to IA responsibilities for the system would also sign the agreement upon their appointment.

Our Response

Comments from the Chief, Operations Division, were responsive; therefore, no further comments were required.

B.5. We recommend that the Commander and District Engineer, Portland District, in coordination with the Operations Project Manager for ~~(b)(3) 10 USC 130e (USACE)~~ validate whether all personnel with logical access to the generic data acquisition control system were approved access based on documentation that demonstrates their justification and need-to-know, in accordance with U.S. Army Corps of Engineers Portland District, "Hydropower Plant Cyber Security Policy for Industrial Control Systems," January 2012, requirements.

USACE Comments

~~(FOUO)~~ ~~(b)(3) 10 USC 130e (USACE)~~


Our Response

Comments from the Chief, Operations Division, were responsive; however, they did not include a completion date for ~~(b)(3) 10 USC 130e (USACE)~~

 Therefore, we request that the Commander

and District Engineer, Portland District, provide the completion date for the planned actions.

~~(FOUO)~~ B.6. We recommend that the Commander and District Engineer, Portland District, in coordination with the Operations Project Managers for ~~(b)(3) 10 USC 130e (USACE)~~, strictly limit physical access to the control rooms where the Willamette Valley supervisory control and data acquisition system and generic data acquisition and control system reside to only personnel with a validated need for access to a controlled area, instead of allowing access to all Government personnel.


USACE Comments

~~(FOUO)~~ The Chief, Operations Division, agreed, stating that the risk assessment methodology for dams resulted in installing access control and monitoring devices at doors to the powerhouse and control room at ~~(b)(3) 10 USC 130e (USACE)~~
~~(b)(3) 10 USC 130e (USACE)~~

Our Response

~~(FOUO)~~ Comments from the Chief, Operations Division, were partially responsive to the intent of the recommendation. We commend the Portland District for taking steps to ensure that the access control and monitoring devices are fully functioning at ~~(b)(3) 10 USC 130e (USACE)~~ to limit access to the control room and for procuring additional devices to further protect the server room at ~~(b)(3) 10 USC 130e (USACE)~~

(b)(3) 10 USC 130e (USACE)




B.7. We recommend that the Commander and District Engineer, Seattle District, in coordination with the Operations Project Manager for (b)(3) 10 USC 130e (USACE) :

~~(FOUO)~~ a. Strictly limit physical access to the control room where the generic data acquisition control system resides to only personnel with a validated need for access to a controlled area instead of allowing access to all Government personnel.

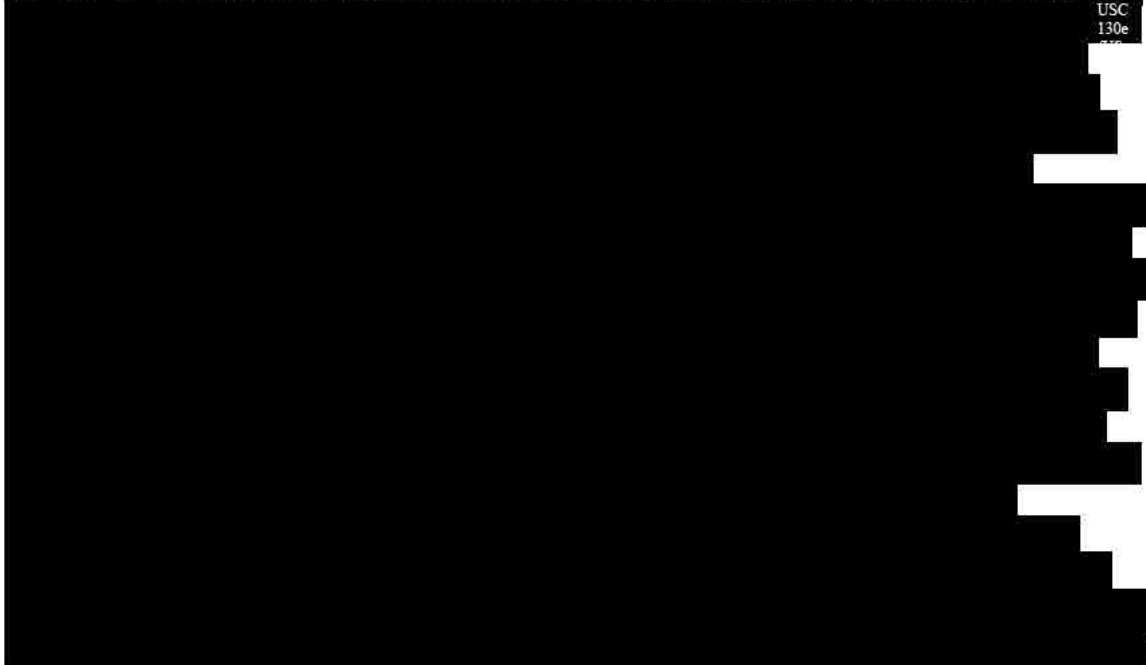
USACE Comments

~~(FOUO)~~ The Chief, Operations Division, agreed, stating that the OPM for (b)(3) 10 USC 130e (USACE) was in the best position to limit access to the control room to only those with a need for access. (b)(3) 10 USC 130e (USACE)



Our Response

~~(FOUO)~~ Comments from the Chief, Operations Division, were partially responsive. (b)(3) 10 USC 130e (USACE)



(FOUO)

(b)(3) 10 USC 130e (USACE)

By limiting proximity card access to only (b)(3) 10 USC 130e (USACE)

We understand that other project personnel, such as those performing administrative, general maintenance, and technical support, may need access to the control room, but they could be granted provisional access and escorted while in the control room when the need arose. Therefore, we request that the Commander and District Engineer, Seattle District, reconsider his position about limiting who is given proximity card access to the control room and provide comments on the final report by February 13, 2013.

b. Validate whether all personnel with logical access to the generic data acquisition control system have signed and approved documentation demonstrating their justification and need-to-know in accordance with U.S. Army Corps of Engineers, Seattle District, "Cyber Security Policy," July 1, 2011, requirements.

USACE Comments

(FOUO) The Chief, Operations Division, agreed, (b)(3) 10 USC 130e (USACE)

Our Response

Comments from the Chief, Operations Division, were responsive; however, they did not include a completion date for when personnel with logical access to GDACS would complete the required documentation to substantiate their need for access. Therefore, we request that the Commander and District Engineer, Seattle District, provide the completion date for the planned actions.

B.8. We recommend that the Commanders and District Engineers, Portland and Seattle Districts, review the performance of the Operations Project Managers related to information assurance control weaknesses and, based on the results, consider corrective actions, as appropriate, to ensure that the industrial control systems are protected by layered, defense-in-depth protection measures defined in DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003.

USACE Comments

(FOUO) The Chief, Operations Division, disagreed, stating that affixing blame and recommending personnel actions overextended our role of identifying deficiencies and

(FOUO) required remedies. He stated that the OPM's performance, as for all personnel, would continue to be assessed annually based on new and developing requirements of the positions, such as those resulting from our audit recommendations.

Our Response

Comments from the Chief, Operations Division, were nonresponsive to the intent of our recommendation. Recommending actions to hold personnel accountable for their actions or inaction is not an overextension of our responsibilities. DoD Directive 5106.01, "Inspector General of the Department of Defense," April 20, 2012, requires the DoD Office of Inspector General, among other responsibilities, to perform audits and make recommendations for corrective action for all matters related to the economy and efficiency of DoD programs and operations. Because the OPMs are ultimately responsible for all aspects of operations that affect their projects, their performance in relation to the existence of significant physical and cyber security weaknesses needs to be reviewed to ensure those types of weaknesses are prevented in the future. Therefore, we request that the Commanders and District Engineers, Portland and Seattle Districts, reconsider their positions to review the OPM's performance related to the existence of the physical and cyber security weaknesses and provide comments on the final report by February 13, 2013.

Finding C. ICSs Were Not Properly Managed to Limit Cyber Security Risks

Personnel from the USACE, Office of Corporate Information (Information Technology), did not effectively manage cyber security risks affecting the USACE information technology portfolio because they did not verify whether Commanders and District Engineers registered all ICSs and certified and accredited those systems in accordance with DoDI 8510.01, "DoD Information Assurance Certification and Accreditation Process (DIACAP)," November 28, 2007. (b)(3) 10 USC 130e (USACE)

[REDACTED]

Systems Used to Operate Critical Infrastructure Were Not Always Certified and Accredited

(FOUO) Personnel in the USACE, Office of Corporate Information (Information Technology), did not effectively manage cyber security risks affecting the USACE information technology portfolio. (b)(3) 10 USC 130e (USACE)

[REDACTED]

(b)(3) 10 USC 130e (USACE)

[REDACTED]


Although Commanders and District Engineers were individually responsible for systems under their purview, the USACE, Office of Corporate Information (Information Technology), was ultimately responsible for the overall USACE information technology portfolio.

systems. However, DoD Directive 8500.01E, "Information Assurance," October 24, 2002, specifically includes stand-alone systems and closed network enclaves as information systems. Although Commanders and District Engineers were individually responsible for

systems under their purview, the USACE, Office of Corporate Information (Information Technology), was ultimately responsible for the overall USACE information technology portfolio. The Office of Corporate Information (Information Technology) developed multiple policies to assist Commanders and District Engineers in managing ICSs and cyber security risks to those systems, but did not provide adequate oversight to ensure

that commanders took appropriate actions to comply with those requirements.¹⁹ Of the three ICSs used to operate the five projects we visited, only the Willamette Valley SCADA system and GDACS were included in the Army Portfolio Management System.²⁰

~~(FOUO)~~ The Portland District, specifically the Hydroelectric Design Center, took appropriate action to manage cyber security risks by certifying and accrediting GDACS in accordance with DoDI 8510.01. ^{(b)(3) 10 USC 130e (USACE)}



Actions Taken to Manage Cyber Security Risks for All ICSs Used to Operate Critical Infrastructure

On February 15, 2012, the USACE Deputy Chief of Engineers issued Operations Order 2012-14, "Federal Information Security Management Act Compliance for Supervisory Control and Data Acquisition Systems, Industrial or Electronic Control Systems, Data Acquisition and Monitoring Systems." This Operations Order requires major subordinate commanders to identify and register all information systems supporting water control, navigation, and hydropower generation in the Army Portfolio Management System. In addition, the Operations Order requires major subordinate commanders to identify risks and reduce cyber vulnerabilities by accrediting those systems in accordance with DoDI 8510.01 requirements. These actions, if implemented, should improve USACE's ability to manage cyber-related risks. As of June 2012, the USACE, Office of Corporate Information (Information Technology), reported that 16 districts identified 24 ICSs and began to certify and accredit those systems. Therefore, the USACE Chief Information Officer should monitor certification and accreditation actions through the use of a plan of actions and milestones to validate whether district commanders completed required actions in accordance with Operations Order 2012-14 timelines.

¹⁹ Memorandum for USACE Regional Information Officers, "USACE SCADA and Electronic Control Systems Consolidated Requirements," January 8, 2010, and "Cyber Security Certification and Accreditation of SCADA Networks and Computing Resources," March 29, 2010.

²⁰ ~~(FOUO)~~ ^{(b)(3) 10 USC 130e (USACE)}



Management Comments on the Finding and Our Response

Summaries of management comments on the finding and our response are in Appendix C.

Recommendations, Management Comments and Our Response

C. We recommend that the Deputy Chief of Engineers, U.S. Army Corps of Engineers, monitor certification and accreditation actions through the use of a plan of actions and milestones to validate whether District Commanders completed required actions in accordance with Operations Order 2012-14, “Federal Information Security Management Act Compliance for Supervisory Control and Data Acquisition Systems, Industrial or Electronic Control Systems, Data Acquisition and Monitoring Systems,” February 15, 2012, timelines.

USACE Comments

The Chief, Operations Division, agreed with the recommendation.

Our Response

Comments from the Chief, Operations Division, were responsive to the intent of our recommendation; however, although he agreed with the recommendation, he did not provide planned actions and the completion date for corrective actions. Therefore, we request that the Deputy Chief of Engineers provide comments on the final report by February 13, 2013.

Appendix A. Scope and Methodology

We conducted this performance audit from January 2012 through September 2012 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

We visited Headquarters, USACE, in Washington, D.C.; the USACE Portland District Office in Portland, Oregon; and the USACE Seattle District Office in Seattle, Washington. In addition, we visited and conducted walkthroughs at (b)(3) 10 USC 130e (USACE)

Washington; to review and test physical security measures that USACE had implemented to detect and protect against unauthorized access to critical infrastructure. Specifically, we reviewed whether those structures implemented the USACE-developed "Baseline Security Posture Guide for Civil Works Projects," December 10, 2004, physical security requirements as well as select physical security requirements defined in Army Regulation 190-13, "The Army Physical Security Program," February 25, 2011, and Army Regulation 190-51, "Security of Unclassified Army Property (Sensitive and Nonsensitive)," September 30, 1993.

We interviewed personnel in the Portland and Seattle Districts, including the Chiefs of the Security and Law Enforcement Offices, security specialists, security managers, park rangers, key custodians, contract security guards, operators, and the Deputies and OPMs for the five projects visited. These personnel were responsible for implementing security requirements, providing day-to-day security, and correcting physical security weaknesses affecting the critical infrastructure. We also interviewed supervisory program analysts, administrative officers, and the Deputies and OPMs for the five projects to determine the process for identifying and budgeting for physical security requirements.

~~(FOUO)~~ We reviewed and tested whether the OPMs, system administrators, and the GDACS Maintenance Team implemented 26 nonstatistically selected DoDI 8500.2 mission assurance category II IA controls based on their criticality in preventing unauthorized physical and cyber access to the ICSs used to operate five critical infrastructure projects. (b)(3) 10 USC 130e (USACE)

~~(FOUO)~~ We interviewed personnel in the Portland and Seattle Districts, including system administrators, the GDACS IA manager, the GDACS IA security officer, the Seattle District Chief of Project Support, system control craftsmen, and Reliability Compliance Coordinators. These personnel were responsible for managing system risk and authorizing and controlling logical access to the Willamette Valley SCADA system, GDACS, and the PLC-based information system. We also interviewed those personnel to determine whether they implemented security devices and configured security settings in accordance with DISA STIGs, and identified and mitigated vulnerabilities affecting the security posture of each information system. In addition, we interviewed supervisory program analysts, administrative officers, the GDACS IA manager for (b)(3) 10 USC 130e (USACE), and the Deputies and OPMs for the five projects to determine the process for identifying and budgeting for IA requirements.

Further, we interviewed the Program Manager at the USACE, Office of Homeland Security, Critical Infrastructure Protection and Resilience Program, to determine how USACE identified, prioritized, and protected critical infrastructure. We also interviewed the USACE, Civil Works, Hydropower Business Line Manager to identify the critical infrastructure that produces hydroelectric power and to determine whether those projects were required to implement additional physical security measures. In addition, we interviewed the Office of Corporate Information (Information Technology) IA Program Manager, Enterprise Services Division, to determine whether USACE maintained an information technology portfolio that contained SCADA systems and to determine whether those systems had been certified and accredited in accordance with DoDI 8510.01, "DoD Information Assurance Certification and Accreditation Process (DIACAP)," November 28, 2007, requirements.

~~(FOUO)~~ We obtained and reviewed site security plans, policies and procedures addressing physical security and access to the projects, and memorandums designating MEVAs and restricted areas at the five projects. (b)(3) 10 USC 130e (USACE)

In addition, we obtained and reviewed North American Electric Reliability Corporation Critical Infrastructure Protection standards addressing cyber security protection requirements to determine the scope of the eight controls (b)(3) 10 USC 130e (USACE) were required to meet. We also obtained and reviewed policies and

procedures that the Portland and Seattle Districts and projects developed to control logical access to the ICSs. Additionally, we obtained and reviewed documentation identifying personnel with logical access to each information system and the control rooms or sensitive areas where the ICSs resided. We used this documentation to determine whether the projects limited access to the ICSs to only personnel with a need-to-know.

~~(FOUO)~~ Further, we obtained and reviewed appointment letters for personnel performing IA responsibilities; network diagrams; and baselines defining ports, protocols, and services supporting ^{(b)(3) 10 USC 130e (USACE)} [REDACTED]

Use of Computer-Processed Data

We relied on computer-processed data generated by the Department of Homeland Security Consequence Top Screen Portfolio Prioritization Tool, which is a web-based tool used by dam owners for establishing the criticality of water control structures in the Dams sector. ^{(b)(3) 10 USC 130e (USACE)} [REDACTED]

Use of Technical Assistance

^{(b)(3) 10 USC 130e (USACE)} [REDACTED]

Prior Coverage

^{(b)(3) 10 USC 130e (USACE)} [REDACTED]


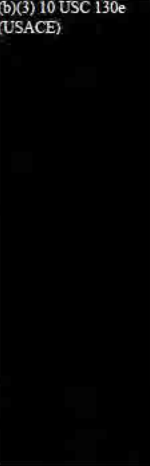

Appendix B. IA Controls Reviewed

The table describes the 26 DoDI 8500.2 IA controls and the results of testing the implementation of those controls over the Willamette Valley (b)(3) 10 USC 130e (USACE)

Specifically, we found significant weaknesses in how 17 of 26 IA controls were implemented. Because two of the three systems were used to operate multiple projects, we identified the results by project.

Table. Results of Testing 26 IA Controls at Projects in the Portland and Seattle Districts

DoDI 8500.2 Control Number	Control Description	(FOUO) Projects With Significant Weaknesses	Audit Finding
DCCT-1: Compliance Testing	A comprehensive set of procedures is implemented that tests all patches, upgrades, and new automated information system applications before deployment.	(FOUO) (b)(3) 10 USC 130e (USACE)	(b)(3) 10 USC 130e (USACE)
ECID-1: Host Based IDS	Host-based IDSs are deployed for major applications and for network management assets, such as routers, switches, and domain name servers.	(FOUO) (b)(3) 10 USC 130e (USACE)	(b)(3) 10 USC 130e (USACE)
PEVC-1: Visitor Control to Computing Facilities	Current signed procedures exist for controlling visitor access and maintaining a detailed log of all visitors to the computing facility.	(b)(3) 10 USC 130e (USACE)	(b)(3) 10 USC 130e (USACE)
ECVP-1: Virus Protection	All servers, workstations, and mobile computing devices implement virus protection that includes a capability for automatic updates.	(FOUO) (b)(3) 10 USC 130e (USACE)	(b)(3) 10 USC 130e (USACE)
PEPS-1: Physical Security Testing	A facility penetration testing process is in place that includes periodic, unannounced attempts to penetrate key computing facilities.	(FOUO) (b)(3) 10 USC 130e (USACE)	(b)(3) 10 USC 130e (USACE)
PECF-1: Access to Computing Facilities	Only authorized personnel with a need-to-know are granted physical access to computing facilities that process sensitive information or unclassified information that has not been cleared for release.	(FOUO) (b)(3) 10 USC 130e (USACE)	(b)(3) 10 USC 130e (USACE)
DCPB-1: IA Program and Budget	A discrete line item for IA is established in programming and budget documentation.	(FOUO) (b)(3) 10 USC 130e (USACE)	(b)(3) 10 USC 130e (USACE)

DoDI 8500.2 Control Number	Control Description	(FOUO) Projects With Significant Weaknesses	Audit Finding
DCSD-1: IA Documentation	All appointments to required IA roles are established in writing, including assigned duties and appointment criteria, such as training, security clearance, and information technology designation. A system security plan is established that describes the technical, administrative, and procedural IA program and policies that govern the DoD information system, and identifies all IA personnel and specific IA requirements and objectives.	(FOUO) (b)(3) 10 USC 130e (USACE) 	(b)(3) 10 USC 130e (USACE) 
IAIA-1: Individual Identification and Authentication	<p>DoD information system access is gained by presenting an individual identifier and password. For systems using logon identification as the individual identifier, passwords are, at a minimum, a case-sensitive, 8-character mix of uppercase letters, lowercase letters, numbers, and special characters, including at least one of each. At least four characters must be changed when a new password is created.</p> <p>Deployed systems with limited data input capabilities implement the password to the extent possible. Registration to receive a user identification and password includes authorization by a supervisor, and is done in person before a designated registration authority.</p> <p>Additionally, to the extent system capabilities permit, system mechanisms are implemented to enforce automatic expiration of passwords and to prevent password reuse. All factory set, default or standard-user identifications and passwords are removed or changed.</p> <p>Authenticators are protected commensurate with the classification or sensitivity of the information accessed; they are not shared; and they are not embedded in access scripts or stored on function keys. Passwords are encrypted both for storage and for transmission.</p>	(FOUO) (b)(3) 10 USC 130e (USACE) 	

DoDI 8500.2 Control Number	Control Description	(FOUO) Projects With Significant Weaknesses	Audit Finding
DCPP-1: Ports, Protocols, and Services	DoD information systems comply with DoD ports, protocols, and services guidance. Automated information system applications, outsourced information technology-based processes, and platform information technology identify the network ports, protocols, and services they plan to use as early in the life cycle as possible and notify hosting enclaves. Enclaves register all active ports, protocols, and services in accordance with DoD and DoD Component guidance.	(FOUO) (b)(3) 10 USC 130e (USACE) [REDACTED]	(b)(3) 10 USC 130e (USACE)
EBVC-1: Virtual Private Network Controls	All virtual private network traffic is visible to a network IDS.	(b)(3) 10 USC 130e (USACE) [REDACTED]	
DCID-1: Interconnection Documentation	For automated information system applications, a list of all hosting enclaves is developed and maintained along with evidence of deployment planning and coordination and the exchange of connection rules and requirements. For enclaves, a list of all hosted automated information system applications, interconnected outsourced information technology-based processes, and interconnected information technology platforms is developed and maintained along with evidence of deployment planning and coordination and the exchange of connection rules and requirements.	(b)(3) 10 USC 130e (USACE) [REDACTED]	
IAAC-1: Account Control	A comprehensive account management process is implemented to ensure that only authorized users can gain access to workstations, applications, and networks and that individual accounts designated as inactive, suspended, or terminated are promptly deactivated.	(FOUO) (b)(3) 10 USC 130e (USACE) [REDACTED]	(b)(3) 10 USC 130e (USACE)
ECPA-1: Privileged Account Control	All privileged user accounts are established and administered in accordance with a role-based access scheme that organizes all system and network privileges into roles. The IA manager tracks privileged role assignments.	(b)(3) 10 USC 130e (USACE) [REDACTED]	

DoDI 8500.2 Control Number	Control Description	(FOUO) Projects With Significant Weaknesses	Audit Finding
VIVM-1: Vulnerability Management	A comprehensive vulnerability management process that includes the systematic identification and mitigation of software and hardware vulnerabilities is in place. Wherever system capabilities permit, mitigation is independently validated through inspection and automated vulnerability assessment or state management tools. Vulnerability assessment tools have been acquired, personnel have been appropriately trained, procedures have been developed, and regular internal and external assessments are conducted. For improved interoperability, preference is given to tools that express vulnerabilities in the Common Vulnerabilities and Exposures naming convention and use the Open Vulnerability Assessment Language to test for the presence of vulnerabilities.	(FOUO) (b)(3) 10 USC 130e (USACE) [REDACTED]	(b)(3) 10 USC 130e (USACE)
EBRP-1: Remote Access for Privileged Functions	Remote access for privileged functions is discouraged, is permitted only for compelling operational needs, and is strictly controlled. Sessions employ security measures, such as a virtual private network with blocking mode enabled. A complete audit trail of each remote session is recorded, and the information assurance manager or information assurance officer reviews the log for every remote session.	(b)(3) 10 USC 130e (USACE) [REDACTED]	
ECMT-1: Conformance Monitoring and Testing	Conformance testing that includes periodic, unannounced, indepth monitoring and provides for specific penetration testing to ensure compliance with all vulnerability mitigation procedures, such as the DoD IAVA or other DoD IA practices is planned, scheduled, and conducted. Testing is intended to ensure that the system's IA capabilities continue to provide adequate assurance against constantly evolving threats and vulnerabilities.	(FOUO) (b)(3) 10 USC 130e (USACE) [REDACTED]	(b)(3) 10 USC 130e (USACE)

~~FOR OFFICIAL USE ONLY~~

DoDI 8500.2 Control Number	Control Description	(FOUO) Projects With Significant Weaknesses	Audit Finding
PRNK-1: Access to Need-to-Know Information	Only individuals who have a valid need-to-know that is demonstrated by assigned official Government duties and who satisfy all personnel security criteria are granted access to information with special protection measures or restricted distribution as established by the information owner.	(b)(3) 10 USC 130e (USACE) [REDACTED]	
ECIC-1: Interconnections among DoD Systems and Enclaves	Discretionary access controls are a sufficient IA mechanism for connecting DoD information systems operating at the same classification, but with different need-to-know access rules. A controlled interface is required for interconnections among DoD information systems operating at different classifications levels or between DoD and non-DoD systems or networks. Controlled interfaces are addressed in separate guidance.	(b)(3) 10 USC 130e (USACE) [REDACTED]	
IAGA-1: Group Identification and Authentication	Group authenticators for application or network access may be used only in conjunction with an individual authenticator. Any use of group authenticators not based on the DoD Public Key Infrastructure has been explicitly approved by the Designated Accrediting Authority.	(FOUO) (b)(3) 10 USC 130e (USACE) [REDACTED]	(b)(3) 10 USC 130e (USACE)
PEPF-1: Physical Protection of Facilities	Every physical access point to facilities housing workstations that process or display sensitive information or unclassified information that has not been cleared for release is controlled during working hours and guarded or locked during nonworking hours.	(FOUO) (b)(3) 10 USC 130e (USACE) [REDACTED]	(b)(3) 10 USC 130e (USACE)
EBRU-1: Remote Access for User Functions	All remote access to DoD information systems, including telework access, is mediated through a managed access control point, such as a remote access server in a demilitarized zone. Remote access always uses encryption to protect the confidentiality of the session. Authenticators are restricted to those that offer strong protection against spoofing. Information regarding remote access mechanisms is protected.	(b)(3) 10 USC 130e (USACE) [REDACTED]	

~~FOR OFFICIAL USE ONLY~~

DoDI 8500.2 Control Number	Control Description	(FOUO) Projects With Significant Weaknesses	Audit Finding
PRAS-1: Access to Information	Individuals requiring access to sensitive information are processed for access authorization in accordance with DoD personnel security policies.	(b)(3) 10 USC 130e (USACE) [REDACTED]	
ECSC-1: Security Configuration Compliance	For enclaves and automated information system applications, all DoD security configuration or implementation guides have been applied.	(FOUO) (b)(3) 10 USC 130e (USACE) [REDACTED]	(b)(3) 10 USC 130e (USACE)
PRRB-1: Security Rules of Behavior or Acceptable Use Policy	A set of rules that describe the IA operations of the DoD information system and clearly delineate IA responsibilities and expected behavior of all personnel is in place. The rules include the consequences of inconsistent behavior or noncompliance. Signed acknowledgment of the rules is a condition of access.	(FOUO) (b)(3) 10 USC 130e (USACE) [REDACTED]	(b)(3) 10 USC 130e (USACE)
EBBD-2: Boundary Defense	Boundary defense mechanisms including firewalls and network IDSs, are deployed at the enclave boundary to the wide area network at layered or internal enclave boundaries and at key points in the network, as required. All Internet access is proxied through Internet access points that are under the management and control of the enclave and are isolated from other DoD information systems by physical or technical means.	(FOUO) (b)(3) 10 USC 130e (USACE) [REDACTED]	(b)(3) 10 USC 130e (USACE)

Appendix C. USACE Comments on the Findings and Our Response

The Chief, Operations Division, USACE, Civil Works, provided comments that incorporated individual comments from the Northwestern Division, Office of Homeland Security, Office of Corporate Information (Information Technology), Operational Protection Division, and National Hydropower Business Line manager. The comments pertained to all sections of the report; they were not always specific to each of the three findings.

USACE Comments on the Report Title

The Chief, Operations Division, stated the title of the report, “USACE, Civil Works, Critical Infrastructure and Industrial Control Systems in the Northwestern Division Were Not Always Protected,” was a conclusion and was not consistent with the subject of the audit announcement memorandum. In addition, he stated that the report title was inflammatory and sensational.

Our Response

We disagree that the report title was inflammatory and sensational. The physical and cyber security weaknesses discussed in the report supported the overall summarization that critical infrastructure and ICSs were not always protected. However, we revised the title to limit the amount of unwanted attention that it might bring from criminals, terrorists, or cyber attackers.

USACE Comments on the Conclusions Related to the Consequence Assessment Reports

The Chief, Operations Division, stated that the consequences (loss of life and economic impacts) described in the report were not the combined impacts associated with the disruption or failure of a project from either a physical or cyber attack. He pointed out that the human health and economic consequences included in the USACE Consequence Assessment Reports for the five projects were based on a “worst reasonable case” for criticality screening purposes. He asked that we clarify the report to show that these consequences represented the highest possible impacts associated with severe damage or disruption at the five projects no matter how the disruption occurred.

Our Response

~~(FOUO)~~ We agree that the overall magnitude of potential economic damages and lost lives, when combined for the five projects, could occur only if a total disruption or failure occurred at each project. We updated the report to more accurately reflect that condition related to the potential that as many as ^{(b)(3) 10 USC 130e (USACE)} [REDACTED]

USACE Comments on Implementing Physical Security Requirements

The Chief, Operations Division, stated that the discussion related to the initial physical security assessments that the USACE Office of Homeland Security conducted using the risk assessment methodology for dams and USACE's transition to implementing security based on Baseline Security Posture requirements was misleading. He asked that we add details to further describe the process. He also asked that we update the report to describe that, on the basis of the recommendations from the risk assessment methodology for dams, USACE implemented a "program pause" to assess the effects of physical security upgrade costs at the 85 projects. In addition, he stated that the issuance of the "Baseline Security Posture Guide" was an alternative approach for implementing security upgrades at the remaining 178 projects that did not upgrade security based on recommendations included in the initial risk assessment methodology for dams.

The Chief, Operations Division, also stated that we incorrectly assessed all five projects against Baseline Security Posture Level II security requirements. Specifically, he stated that (b)(3) 10 USC 130e (USACE) implemented security upgrades based on recommendations from the risk assessment methodology for dams; (b)(3) 10 USC 130e (USACE) implemented security upgrades based on the Northwestern Division Appendix B, "Definition of Physical Security Packages," January 14, 2004; and (b)(3) 10 USC 130e (USACE) implemented security upgrades based on a Baseline Security Posture Level I designation. Therefore, he stated that (b)(3) 10 USC 130e (USACE) was required to implement only the seven Baseline Security Posture Level I security requirements.

(FOUO)


(b)(3) 10 USC 130e (USACE)

Our Response

It was not our intent to provide misleading information about USACE actions to secure critical infrastructure projects. We understand that the OPMs for the five projects included in the scope of the audit implemented physical security upgrades based on different criteria. Therefore, we revised the report to clearly distinguish how the criticality of each project was assessed and how those projects then implemented additional physical security measures to improve the overall strength of each project's security posture. We described the general process included in USACE-provided documentation as well as details explained by the Program Manager, Critical Infrastructure Protection and Resilience Program, Office of Homeland Security. The information included in the background section of the report was not intended to describe

the entire history of USACE actions to secure its critical infrastructure. However, we included additional details to more clearly describe the overall process, to include the genesis of the alternative methods for upgrading security at the five projects in the Northwestern Division. In addition, we specifically identified how security upgrades were initially implemented at each project.

Although the initial assessments (risk assessment methodology for dams, the Baseline Security Posture, or the Northwestern Division Appendix B) that defined what type of security upgrades were needed to adequately protect the five structures from terrorist or criminal activity are essential to understanding the process through which USACE implemented additional security, it is equally critical to evaluate the security posture of those structures based on the security requirements that should have been implemented at the time of the audit. (b)(3) 10 USC 130e (USACE)



USACE Comments on Current Physical Security Requirements

The Chief, Operations Division, pointed out that using the Baseline Security Posture strategy and applicable requirements ended in 2008, when the Critical Infrastructure Protection and Resilience Program implemented a different portfolio risk assessment framework to address security risks at projects. He stated that guidance to implement the new strategy of mitigating security risks was defined in Chapter 23, “Physical Security of Dams,” of Engineering Regulation 1110-2-1156, “Engineering and Design Safety of Dams – Policy and Procedures,” October 28, 2011. He also stated that the current process would support risk-informed decisions that took into account a wide spectrum of consequences, vulnerabilities, and threats to critical projects in the USACE portfolio. As such, the Chief, Operations Division, suggested that we update the recommendations related to implementing physical security requirements based on the guidance in Chapter 23 of Engineering Regulation 1110-2-1156.

Our Response

During the audit, USACE did not provide Engineering Regulation 1110-2-1156, and personnel in the Portland and Seattle Districts did not identify this document as their overarching policy for implementing physical security requirements. Based on USACE comments, we obtained and reviewed Chapter 23 of Engineering Regulation 1110-2-1156. Chapter 23 requires all USACE dams to maintain an adequate security posture to ensure that projects are operated in a safe and secure manner. Additionally, it requires all

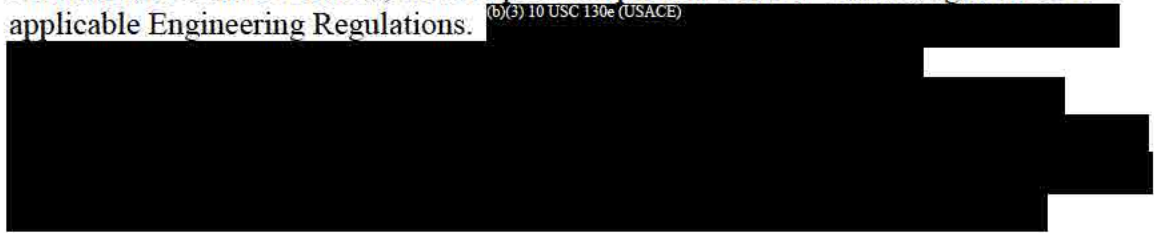
dams to implement a physical security program that includes developing a project-specific physical security plan, conducting physical security inspections, and implementing security systems appropriately designed and constructed in accordance with Army Regulation 190-11, "Physical Security of Arms, Ammunition, and Explosives," November 15, 2006, and Army Regulation 190-13. Although the Office of Homeland Security stated that it requires Commanders and District Engineers to implement requirements defined in Chapter 23 for mitigating physical security risks, it does not identify specific physical security requirements that the projects must implement. Additionally, the Security Officer, Security and Law Enforcement Offices, Portland and Seattle Districts, stated that the projects under their purview still implemented physical security requirements defined in the "Baseline Security Posture Guide." Therefore, we did not revise the recommendation to require the projects to implement security requirements in accordance with Chapter 23 of Engineering Regulation 1110-2-1156.

USACE Comments on Funding Physical Security Requirements

The Chief, Operations Division, disagreed that Commanders and District Engineers were not recognizing the criticality of security shortfalls. In particular, the comments from the Northwestern Division stated that the Portland District officials prioritized funding appropriately and consistently with defensible business models. In addition, he stated that the prioritization and ranking of project security requirements is defined in yearly updates to Engineering Circular 11-2-202, "Army Programs, Corps of Engineers Civil Works Direct Program, Program Development Guidance, FY 2014."²¹ Further, he stated that Engineering Circular 11-2-202 generally ranks security needs lower than project (mission) requirements because of limited operation and maintenance funds. Consequently, he stated, the Engineering Circular may have necessitated that the OPMs or security managers rank security needs lower on their list of priorities. As such, he asked that we further describe whether the OPMs followed the guidance described in Engineering Circular 11-2-202 to show that if they did follow it, certain security upgrades could have been funded.

Our Response

~~(FOUO)~~ We understand that project OPMs and the Commanders and District Engineers, Portland and Seattle Districts, were required to prioritize needs based on guidance in applicable Engineering Regulations. ^{(b)(3) 10 USC 130e (USACE)}



²¹ Budget guidance for FY 2011 was established in Engineering Circular 11-2-194, "Army Programs, Corps of Engineers Civil Works Direct Program, Program Development Guidance, FY 2011," April, 1, 2009, and guidance for FY 2012 was established in Engineering Circular 11-2-199, "Army Programs, Corps of Engineers Civil Works Direct Program, Program Development Guidance, FY 2012," March 31, 2010.

(FOUO)

(b)(3) 10 USC 130e (USACE)

(FOUO) Further, solutions to mitigate physical security weaknesses found during physical security inspections were not always included in the projects' budget submissions.

(b)(3) 10 USC 130e (USACE)

The criticality of security shortfalls was not always recognized because security needs were not consistently included in budget submissions, and when they were, the needs were often not funded because they were always ranked lower than other needs.

USACE Comments on Mission Assurance Category of ICSs

The Chief, Operations Division, stated that it was inaccurate to state that all ICSs used to operate hydropower generation projects were designated mission assurance category II systems. In particular, he stated that USACE designated all networks as mission assurance category II systems. Additionally, he stated that individual systems on the network could be designated as either mission assurance category II or III systems. He asked that we revise the report to state that USACE designated all ICS control networks as mission assurance category II networks.

Our Response

We revised the report to show that USACE generally designated all ICS networks used to operate hydropower projects as mission assurance category II systems that processed sensitive information.

USACE Comments on Vulnerability Assessments

The Chief, Operations Division, stated that we did not define a standard for conducting more frequent vulnerability assessments and we did not define how frequently USACE should conduct those assessments. In addition, he stated that DoD and Army regulations require system owners to certify and accredit systems every 3 years. He also stated that the Federal Information Security Management Act requires annual security testing. Further, he pointed out that vulnerability assessment tools, such as Retina, result in "false

positives” that could have already been mitigated by other controls and documented in the plan of actions and milestones.

Our Response

(FOUO) (b)(3) 10 USC 130e (USACE)
[Redacted]

(FOUO) (b)(3) 10 USC 130e (USACE)
[Redacted]

USACE Comments on the Description of ICSs

The Chief, Operations Division, stated that we incorrectly assumed that all systems not connected to the Internet were stand-alone systems.

Our Response

Although an individual system not connected to the Internet is a stand-alone system, we removed “stand-alone” (b)(3) 10 USC 130e (USACE)
[Redacted] We described the PLC-based information system as a non-Internet-connected system.

USACE Comments on Registration of ICSs in the Army Portfolio Management System

The Chief, Operations Division, stated that the statement in the draft report, “All ICSs were not included in the Army Portfolio Management System because the IA Program Manager stated that USACE defined an information system as one that connects to the

Internet or another system using a routable protocol,” was inaccurate. He stated that the IA Program Manager provided documentation requiring system owners to register ICSs in the Army Portfolio Management System and perform security assessments for the purpose of determining DoD Information Assurance Certification and Accreditation Process compliance. He suggested that we update the report to show that district personnel did not consider ICSs to be information systems that were required to be registered as part of the USACE information technology portfolio.

In addition, he pointed out that ICSs were not managed as part of the USACE information technology portfolio. For example, he stated that ICSs were treated more like DoD weapon systems that were programmed and managed separately from the information technology portfolio. As such, he asked that we revise the report to reflect that ICSs were managed by the Civil Works Directorate and not by the Office of Corporate Information (Information Technology). He also stated that (b)(3) 10 USC 130e (USACE)

Our Response

We revised the report to show who was responsible for registering and taking action to certify and accredit the ICSs and the reasons why those systems were not included in the Army Portfolio Management System. (b)(3) 10 USC 130e (USACE)

We do agree that individual Commanders and District Engineers, as the system owners within the USACE Civil Works Directorate, are responsible for managing and funding ICS functionality and security. However, ICSs are still information systems based on NIST SP 800-82, and therefore, those systems should be managed as part of the USACE information technology portfolio. The Office of Corporate Information (Information Technology) is responsible for overseeing and managing USACE information systems as part of the information technology portfolio.

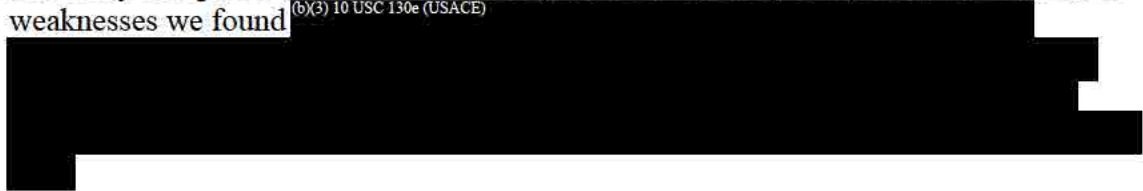
The Office of Corporate Information (Information Technology) issued guidance, including various memorandums and policies, to assist system owners in managing cyber security risks affecting ICSs. Also, the Office of Corporate Information wrote Operations Order 2012-14 that the Deputy Chief of Engineers issued to more effectively manage cyber security risks affecting the ICSs. Operations Order 2012-14 identified the Office of Corporate Information (Information Technology) as the lead for complying with risk management activities. Those activities included reviewing plans of action and milestones and other documentation supporting the certification and accreditation process and advising system owners on how to appropriately mitigate risk. As our results show, Commanders and District Engineers did not always register the ICSs in the Army Portfolio Management System and effectively manage cyber security risks. Including ICSs in the information technology portfolio increases USACE’s ability to ensure that cyber security risks affecting these systems, which are increasingly targets of cyber attackers, are adequately and consistently managed.

USACE Comments on Implementation of Information Assurance Controls

The Chief, Operation Division, USACE, Civil Works, stated that USACE implements security controls outlined in NIST SP 800-53 based on IA controls defined in DoDI 8500.2. He stated that 100-percent implementation of all controls could not occur, and therefore, compensating controls and other alternatives to mitigate risks to an acceptable level of risk based on available funding were needed. Therefore, he stated, implementing security controls was subject to an overall risk mitigation framework. He also stated that USACE used the Defense Information Assurance Certification and Accreditation Process to achieve an acceptable level of risk. He asked us to acknowledge that it was acceptable under a risk mitigation framework for certain security controls to be poor or missing, if documented in a plan of action and milestones.

Our Response

We agree that system owners must make risk-based decisions that include accepting certain levels of risk; however, those decisions must be documented. Throughout the certification and accreditation process for GDACS, the Hydroelectric Design Center documented specific risks that would not be mitigated; the Designated Accrediting Authority accepted those risks when he signed the Authority to Operate. However, the weaknesses we found (b)(3) 10 USC 130e (USACE)



USACE Comments

The Chief, Operation Division, stated that we did not need to attribute the number of dams USACE owned and operated to the Program Manager, Critical Infrastructure Protection and Resilience Program, USACE, Office of Homeland Security.

Our Response

We attributed the number of water structures because the Program Manager, Critical Infrastructure Protection and Resilience Program, did not provide documentation to support the approximately 800 USACE water control structures. On the basis of management comments, we again requested documentation; it showed that USACE owned only 702 water structures. Therefore, we revised the report accordingly.

USACE Comments

The Chief, Operations Division, stated that USACE had an IA program and the Office of Corporate Information (Information Technology) had a budget. He also stated that critical infrastructure projects could or could not have a separate IA budget line item. Accordingly, he asked us to revise the report.

Our Response

We agree that USACE implemented an IA program and understand that the Office of Corporate Information (Information Technology) had a separate IA budget. However, the IA Program Manager, Office of Corporate Information (Information Technology), stated that the IA budget pertained to managing CorpsNet, not ICSs. In addition, personnel responsible for preparing and submitting budget submissions at the five projects and personnel responsible for consolidating and prioritizing those budget submissions in the Portland and Seattle Districts and in the Northwestern Division stated that IA needs to secure ICSs were not submitted as part of the Headquarters, USACE, IA program. Instead, they stated they were required to include those costs in the overall operation and maintenance budget line item. We revised the report accordingly.

Glossary

Accreditation. An official management decision that authorizes an information system to operate at a specific level of risk.

Audit Trail. A record of activity that is maintained to provide a basis for reconstructing or reviewing user activities.

Bulk Electric System. A large interconnected electrical system comprised of generation and transmission facilities and their control systems.

Certification. A comprehensive evaluation and validation process to establish whether an information system complies with required information assurance controls and procedures.

Computing Facility. A room, building, or section of a building that houses key information technology assets, such as servers, network management servers, domain name servers, switches, firewalls, routers, and IDSs, that must be physically protected.

Conformance Testing. A process for determining whether a system meets requirements or specific standards necessary for achieving connectivity or interoperability.

Critical Infrastructure. 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.

Cyber Security. Technology, processes, and practices designed to protect networks, computers, programs, and data from attack, damage, or unauthorized access.

Designated Accrediting Authority. The official with the authority to formally assume responsibility for operating a system at an acceptable level of risk.

Enclave. Collection of computing environments connected by one or more internal networks under the control of a single authority or security policy. These include local area networks and the applications they host, backbone networks, and data processing centers.

Firewall. Hardware and software components that permit authorized users to access and transmit information, as well as deny access to unauthorized users.

Information Assurance (IA). Measures that protect information or an information system's availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

Industrial Control System (ICS). A general term that encompasses several types of control systems, including SCADA systems, distributed control systems, and PLCs.

Information Assurance Manager. The individual responsible for the information assurance program of a DoD information system or organization.

Information Assurance Vulnerability Alert. A comprehensive process that notifies DoD personnel about vulnerabilities affecting their information systems and networks; they include implementation strategies to reduce the risk associated with identified vulnerabilities.

Information System. A set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information.

Information Technology. Any equipment or interconnected system or subsystem used in the automatic acquisition, storage, manipulation, management, movement, control, display, interchange, transmission or reception of data or information.

Interconnection. A direct connection between two or more information systems established for sharing data and other information resources.

Intrusion detection system (IDS). A device that inspects activity occurring within a network or specific host to identify suspicious patterns that could indicate someone is attempting to compromise a system or network.

Logical Access. Technical controls within an information system that limit and control access to data or the information system.

Mission Assurance Category. The classification assigned to DoD information systems, which reflects the importance of information relative to the achievement of DoD goals and objectives, particularly the warfighters' combat mission, and is primarily used to determine the requirements for availability and integrity.

Mission Essential or Vulnerable Area (MEVA). Facilities or areas within an installation that by the nature of the area are vulnerable to theft, trespassing, damage, or other criminal activity; these areas are vital to the mission of the installation.

Need-to-Know. The necessity for access to, or knowledge of, specific DoD information required to carry out official duties.

Network. A group of computers and associated devices connected by communication lines, routers, hubs, and technical control devices.

Operating System. The software that controls the execution of other computer programs, schedules tasks, allocates storage, manages the interface to peripheral

hardware, and presents a default interface to the user when no application program is running.

Port. The logical connection point that enables the transmission of information from computer to computer.

Privileged Access. An authorized user who has access to system control, monitoring, or administration functions that an ordinary user would not have.

Programmable Logic Controller (PLC). A solid-state control system that has user-programmable memory for storing instructions to implement specific functions (for example, input and output control, communication, and data processing).

Protocol. A standard that specifies the format of data as well as the rules to be followed when performing specific functions.

Risk Management. The process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level.

Sensitive Information. Any data in which the loss, misuse, or unauthorized access to, or modification of, could adversely affect our national interests or DoD mission.

Supervisory Control and Data Acquisition (SCADA). A highly distributed system used to control geographically dispersed assets where centralized data acquisition and control are critical.

System Administrator. An individual that is responsible for administering the use of multiuser computer or communications systems.

Threat. A circumstance or event that could adversely impact organizational operations and assets, individuals, other organizations, or the Nation, through an information system by unauthorized access, destruction, disclosure, modification of information, or denial of service.

Vulnerability. The weaknesses in an information system, system security procedures, or internal controls that could be exploited or triggered by the source of a threat.

U.S. Army Corps of Engineers Comments



REPLY TO
ATTENTION OF

DEPARTMENT OF THE ARMY
U.S. ARMY CORPS OF ENGINEERS
441 G STREET, NW
WASHINGTON, DC 20314-1000

CECW-CO

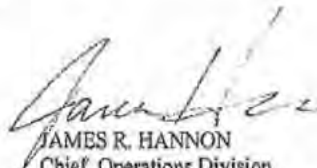
OCT 25 2012

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: U.S. Army Corps of Engineers Response to Draft Audit Report, USACE, Civil Works, Critical Infrastructure and Industrial Control Systems in the Northwestern Division Were Not Always Protected (Project No. D2012-D000LC-0080.000)

1. Reference DoD IG subject report.
2. Attached is the response provided by USACE Headquarters Operations Division, Directorate of Contingency Operations and Homeland Security, Corporate Information, and Northwestern Division to the subject audit draft report. Given the complexity and substantive nature of these comments the USACE Headquarters would be pleased to meet with the report authors prior to finalizing this report.
3. Please feel free to contact [REDACTED] CEIR, who can be reached at [REDACTED] or via email at [REDACTED]

Encl


JAMES R. HANNON
Chief, Operations Division
Directorate of Civil Works

DISTRIBUTION:
COMMANDER, USACE
DEPUTY COMMANDER, USACE
DEPUTY COMMANDING GENERAL FOR CIVIL AND EMERGENCY OPERATIONS
DIRECTOR OF CIVIL WORKS
DIRECTORATE OF CIVIL WORKS, OFFICE OF HOMELAND SECURITY
DIRECTORATE CONTINGENCY OPERATIONS AND HOMELAND SECURITY, DEPUTY
DIRECTORATE CONTINGENCY OPERATIONS AND HOMELAND SECURITY, G2
DIRECTORATE CONTINGENCY OPERATIONS AND HOMELAND SECURITY, G3
COMMAND PROVOST MARSHAL
INTERNAL REVIEW OFFICE, CHIEF
COMMANDER NORTHWESTERN DIVISION
DEPUTY DIVISION COMMANDER NORTHWESTERN DIVISION

CECW-CO

SUBJECT: USACE Response to Audit of the U.S. Army Corps of Engineers, Civil Works,
Information Systems Supporting Critical Infrastructure (Project No. D2012-DOOOLC-0080.000)

US ARMY CORPS OF ENGINEERS PORTLAND DISTRICT

US ARMY CORPS OF ENGINEERS SEATTLE DISTRICT

COMMENT SUBMITTAL FORM

DoD Office of Inspector General Report

USACE, Civil Works, Critical Infrastructure and Industrial Control Systems in the
Northwestern Division Were Not Always Protected
Project No. D2012-D000LC-0080.000

Reviewer Name:

National Program Manager
Critical Infrastructure Protection and Resilience (CIPR) Program
US Army Corps of Engineers, Headquarters
Office of Homeland Security

Email:

Please designate your comment as either: Administrative (e.g., error of fact easily corrected, grammatical error, etc) or Substantive (e.g., major flaw that must be addressed)

Comments on General Document

Comment Number:	1
Page Number:	Title Page
Line Number:	8-11
Comment Type: A: Administrative or S: Substantive	Administrative
Comment: (add additional space if needed)	The title of the report is not consistent with the subject of the audit as presented in the DoD IG audit announcement memorandum, dated 3 January 2011, the Entrance Conference briefing (31 January 2012), and the Exit-Conference briefing (22 June 2012). Current title states an overall conclusion/finding rather than the general subject of the audit.
Recommended Change: (add additional space if needed)	Recommend to modify title to align consistently with subject as: "Audit of the U.S. Army Corps of Engineers, Civil Works, Information Systems Supporting Critical Infrastructure in the Northwestern Division" (Project No. D2012-D000LC-0080.000)

Revised

Comment Number:	2
Page Number:	1
Line Number:	13-15 (left column)
Comment Type: A: Administrative or S: Substantive	Administrative
Comment: (add additional space if needed)	Correct the statement "to secure and protect critical infrastructure and industrial control systems (ICSSs) from physical and cyber threats."
Recommended Change: (add additional space if needed)	Correct to "to secure and protect against unauthorized access to information systems and industrial control systems (ICSSs) supporting critical infrastructure from physical and cyber threats."

Revised

**Final Report
Reference**

Comment Number:	3
Page Number:	I
Line Number:	11-12
Comment Type: A: Administrative or S: Substantive	Substantive
Comment: (add additional space if needed)	(b)(3) 10 USC 130e (USACE)
Recommended Change: (add additional space if needed)	

Page 13

Revised, page 13

Comment Number:	4
Page Number:	ii
Line Number:	20-24
Comment Type: A: Administrative or S: Substantive	Substantive
Comment: (add additional space if needed)	The USACE Baseline Security Posture strategy and associated requirements was completed in FY2008. The portfolio-risk assessment framework currently being implemented by the Critical Infrastructure Protection and Resilience (CIPR) Program to address security risks at our critical projects will help to inform the budgetary security requirements and decisions made by our Commanders to mitigate those risks. Guidance to Division and District personnel on developing proper mitigation and corrective actions resulting from security risk assessments is outlined in Chapter 23 (Physical Security of Dams) as part of Engineering Regulation ER 1110-2-1156, "Engineering and Design Safety of Dams – Policy and Procedures", dated 28 October 2011. This process will support risk-informed decisions considering a wide spectrum of consequences, vulnerabilities, and threats to critical facilities within USACE's portfolio.

**Final Report
Reference**

Recommended Change: (add additional space if needed)	Suggest sentence be updated as follows: "We recommend that the Commanders and District Engineers, Portland and Seattle Districts, in coordination with the OPMs, address physical security requirements in accordance with guidance outlined in Chapter 23 (Physical Security of Dams) as part of Engineering Regulation ER 1110-2-1156, "Engineering and Design Safety of Dams – Policy and Procedures", dated 28 October 2011."
--	---

Comment Number:	5
Page Number:	1
Line Number:	12-13
Comment Type: A: Administrative or S: Substantive	Administrative
Comment: (add additional space if needed)	Delete "According to the USACE Critical Infrastructure Protection and Resilience Program, Program Manager".
Recommended Change: (add additional space if needed)	Edit sentence as follows: "USACE owns and operates approximately 800 water control structures; approximately..."

Comment Number:	6
Page Number:	3
Line Number:	21-23
Comment Type: A: Administrative or S: Substantive	Substantive
Comment: (add additional space if needed)	(b) (5), (b)(3) 10 USC 130e (USACE)
Recommended Change: (add additional space if needed)	

Revised

Page 4

Revised

**Final Report
Reference**

Comment Number:	7
Page Number:	4
Line Number:	24
Comment Type: A: Administrative or S: Substantive	Administrative
Comment: (add additional space if needed)	Wrong ranking number.
Recommended Change: (add additional space if needed)	Change to (b)(3) 10 USC 130e (USACE) ranked 66 th .

Page 5

Revised

Comment Number:	8
Page Number:	12
Line Number:	24-25
Comment Type: A: Administrative or S: Substantive	Administrative
Comment: (add additional space if needed)	Delete "According to the USACE Critical Infrastructure Protection and Resilience Program, Program Manager".
Recommended Change: (add additional space if needed)	Edit sentence as follows: "USACE owns and operates approximately 800 water control structures; approximately..."

Page 14

Revised

Comment Number:	9
Page Number:	38
Line Number:	25
Comment Type: A: Administrative or S: Substantive	Administrative
Comment: (add additional space if needed)	Delete in footnote: "According to the USACE Critical Infrastructure Protection and Resilience Program, Program Manager".
Recommended Change: (add additional space if needed)	Edit sentence as follows: "USACE owns and operates approximately 800 water control structures; approximately..."

Page 55

Deleted and Revised

**Final Report
Reference**

Comment Number:	10
Page Number:	42
Line Number:	8-9
Comment Type: A: Administrative or S: Substantive	Administrative
Comment: (add additional space if needed)	Wrong title (Project Manager vs. Program Manager)
Recommended Change: (add additional space if needed)	Edit sentence as follows: "Further, we interviewed the USACE Office of Homeland Security, Critical Infrastructure Protection and Resilience Program, Program Manager", to determine...

Page 59

Revised

COMMENT SUBMITTAL FORM

DoD Office of Inspector General Report

USACE, Civil Works, Critical Infrastructure and Industrial Control Systems in the
Northwestern Division Were Not Always Protected
Project No. D2012-D000LC-0080.000

Reviewer Name: [REDACTED]
National Hydropower Business Line Manager
Operations Division
US Army, Corps of Engineers, Headquarters

Email: [REDACTED]

Please designate your comment as either: Administrative (e.g., error of fact easily corrected, grammatical error, etc) or Substantive (e.g., major flaw that must be addressed)

Comments on General Document

Comment Number:	1
Page Number:	Title Page
Line Number:	N/A
Comment Type: A: Administrative or S: Substantive	Administrative
Comment: (add additional space if needed)	The main report title is stated as a conclusion of the audit
Recommended Change: (add additional space if needed)	Suggest changing the title to "Audit of USACE Civil Works Critical Infrastructure and Industrial Control Systems in the Northwestern Division"

Revised

Comment Number:	2
Page Number:	1
Line Number:	11 - 13, column 2
Comment Type: A: Administrative or S: Substantive	Substantive
Comment: (add additional space if needed)	Risk consequences are stated in terms of lives lost and economic damages but are not referenced as to how these consequences were derived.
Recommended Change: (add additional space if needed)	The report should state how risk consequences were computed or reference a source for the numbers stated.

COMMENT SUBMITTAL FORM

DoD Office of Inspector General Report

USACE, Civil Works, Critical Infrastructure and Industrial Control Systems in the
Northwestern Division Were Not Always Protected
Project No. D2012-D000LC-0080.000

Reviewer Name: [REDACTED]
National Hydropower Business Line Manager
US Army Corps of Engineers, Headquarters
Operations and Regulatory Division

Email: [REDACTED]

Reviewer Name: [REDACTED]
National Program Manager
Critical Infrastructure Protection and Resilience (CIPR) Program
US Army Corps of Engineers, Headquarters
Office of Homeland Security

Email: [REDACTED]

Comments on Findings and Recommendations
(Supersedes comments submitted prior to 13 Nov 2012)

Recommendation:	B.1
Comment Number:	1
Page Number:	34
Line Number:	14-15
Comment Type: A: Administrative or S: Substantive	Substantive
Comment: (add additional space if needed)	Concur. The USACE Civil Works budget development process currently allows for the consideration of all District and Division funding requirements through a complex prioritization process. USACE Districts and Divisions submit their information assurance funding requirements to HQUSACE Programs Integration Division for further consideration and prioritization against other competing requirements. Regarding information assurance requirements, the HQUSACE Programs Integration Division currently gives separate consideration to information through the Operations Hydropower Business Line budget development process by giving a special budget category to address electric reliability cyber security requirements for each impacted District, as required by Engineering Regulation ER 1130-2-551 "Hydropower Operations and Maintenance Policy Bulk Power System Reliability Compliance Program", dated 30 September 2009, and Engineering Pamphlet EP 1130-2-551 "Hydropower Operations and Maintenance Policy

Revised
Page 43

	<p>Implementation of Bulk Power System Reliability Compliance Program", dated 30 September 2009. These documents outline guidance to Districts and Divisions to establish and maintain a USACE corporate program, the Army Corps of Engineers Compliance and Monitoring Enforcement (ACE-CME) Program, to address compliance with the applicable Federal Energy Regulatory Commission (FERC) approved and pending Bulk Power System (BPS) Reliability Compliance Standards. Since 2009, these cyber security requirements have been fully funded, to include requirements associated with standards CIP-002 to CIP-009 (Cybersecurity Standards).</p> <p>Additionally, the HQUSACE Office of Homeland Security has completed screening the NWD portfolio to help identify and prioritize critical facilities within that MSC. Official results were transmitted to USACE Commanders and staff via Director of Contingency Operations (DCO) memorandum, dated 13 March 2012, and supersedes any previous lists developed. As outlined in the aforementioned memo, this is the initial step in the effective implementation of USACE policy guidance driving USACE's Critical Infrastructure Protection and Resilience (CIPR) portfolio security risk management framework, outlined in Chapter 23 (Physical Security of Dams) as part of Engineering Regulation ER 1110-2-1156 "Engineering and Design Safety of Dams - Policy And Procedures", dated 28 October 2011. USACE has already implemented this security risk process at a top tier of NWD facilities in 2012, which include the 5 facilities addressed in this report. For these 5 critical projects and per guidance outlined in ER 1110-2-1156, security risk assessments were completed and fully documented, vulnerabilities to feasible threat scenarios were identified, and associated protective measures recommended. This information was distributed to Commanders in Seattle and Portland District as required. This information will help inform the budgetary security requirements and decisions made by Commanders to mitigate those risks.</p> <p>The HQUSACE Office of Homeland Security, Operations Division, and Operational Protection Division will be jointly working with the HQUSACE Civil Works Programs Integration Division and HQUSACE Business Line Managers in updating budget development guidance so physical security requirements at critical facilities can be properly incorporated into the FY2015 budget development process.</p>
Recommended Change: (add additional space if needed)	None.

COMMENT SUBMITTAL FORM

DoD Office of Inspector General Report

USACE, Civil Works, Critical Infrastructure and Industrial Control Systems in the
Northwestern Division Were Not Always Protected
Project No. D2012-D000LC-0080.000

Please return to [REDACTED]

Reviewer Name: [REDACTED]

Email: [REDACTED]

Please designate your comment as either: Administrative (e.g., error of fact easily corrected, grammatical error, etc) or Substantive (e.g., major flaw that must be addressed)

Comments on General Document

Comment Number:	1
Page Number:	5
Line Number:	3
Comment Type:	S
Comment: (add additional space if needed)	(b)(3) 10 USC 130e (USACE)
Recommended Change: (add additional space if needed)	

Comment Number:	2
Page Number:	24
Line Number:	16-20
Comment Type:	S
Comment: (add additional space if needed)	(b)(3) 10 USC 130e (USACE)
Recommended Change:	

Office of Corporate
Information
(Information
Technology)
Comments

Revised

Page 33

**Final Report
Reference**

(add additional space if needed)	(b)(3) 10 USC 130e (USACE)
----------------------------------	----------------------------

Comment Number:	3
Page Number:	24
Line Number:	24
Comment Type:	S

Comment: (add additional space if needed)	(b)(3) 10 USC 130e (USACE)
--	----------------------------

Recommended Change: (add additional space if needed)	
--	--

Comment Number:	4
Page Number:	26
Line Number:	11
Comment Type:	S

Comment: (add additional space if needed)	(b)(3) 10 USC 130e (USACE)
--	----------------------------

Recommended Change: (add additional space if needed)	
--	--

Comment Number:	5
Page Number:	38
Line Number:	17-20

Page 33

Revised

Page 34

Revised

Page 55

12

Final Report
Reference

Comment Type:	S
Comment: (add additional space if needed)	(b)(3) 10 USC 130e (USACE)
Recommended Change: (add additional space if needed)	

Comment Number:	6
Page Number:	17
Line Number:	footnote
Comment Type:	s
Comment: (add additional space if needed)	"the overall USACE budget did not include a separate IA budget line;..." There is an IA program in the Corps and it does have a budget within CECI. The critical infrastructure projects themselves may/may not have a separate line item in the project budget
Recommended Change: (add additional space if needed)	Although the USACE budget for the IA program is part of the CECI budget, project budgets did not include a separate line item for IA:"

Comment Number:	7
Page Number:	41

Revised

Page 25

Revised

Page 58

Final Report
Reference

Line Number:	22-23
Comment Type:	S
Comment: (add additional space if needed)	Same as comment number 1 of this document
Recommended Change: (add additional space if needed)	Same as comment number 1 of this document

Revised

Comment Number:	8
Page Number:	23
Line Number:	8-9
Comment Type:	S
Comment: (add additional space if needed)	Same as comment 2
Recommended Change: (add additional space if needed)	Same as comment 2

Page 31

Comment Number:	9
Page Number:	23
Line Number:	10
Comment Type:	S
Comment: (add additional space if needed)	(b)(3) 10 USC 130e (USACE)
Recommended Change: (add additional space if needed)	

Page 31

Comment Number:	10
Page Number:	39
Line Number:	5-6
Comment Type:	S
Comment: (add additional space if needed)	(b)(3) 10 USC 130e (USACE)

Page 56

	(b)(3) 10 USC 130e (USACE), (b) (5)
Recommended Change: (add additional space if needed)	

Comment Number:	11
Page Number:	38
Line Number:	18-19
Comment Type:	S
Comment: (add additional space if needed)	(b)(3) 10 USC 130e (USACE)
Recommended Change: (add additional space if needed)	

Page 55

Comments on Findings and Recommendations

Recommendation:	C
Comment Number:	
Page Number:	
Line Number:	
Comment Type: A: Administrative or S: Substantive	
Comment: (add additional space if needed)	There is no comment from CECI on the actual recommendation itself. CECI concurs as written.
Recommended Change: (add additional space if needed)	

COMMENT SUBMITTAL FORM

DoD Office of Inspector General Report

USACE, Civil Works, Critical Infrastructure and Industrial Control Systems in the
Northwestern Division Were Not Always Protected
Project No. D2012-D000LC-0080.000

Please return to [REDACTED]

Reviewer Name: Operational Protection Division (OPD)

[REDACTED]

Email: [REDACTED]

Please designate your comment as either: Administrative (e.g., error of fact easily corrected, grammatical error, etc) or Substantive (e.g., major flaw that must be addressed)

Comments on General Document

Comment Number:	1
Page Number:	Pg i thru 15 and other locations throughout the report
Line Number:	Pg i, Lines 6 thru 25 and other locations throughout the report
Comment Type: A: Administrative or S: Substantive	S: Substantive
Comment: (add additional space if needed)	(b)(3) 10 USC 130e (USACE) [REDACTED]
Recommended Change: (add additional space if needed)	[REDACTED]

Pages i thru 23

Revised

**Final Report
Reference**

	(b)(3) 10 USC 130e (USACE)
--	----------------------------

Comment Number:	2
Page Number:	i
Line Number:	Lines 17-21, and other locations throughout the report
Comment Type: A: Administrative or S: Substantive	S: Substantive
Comment: (add additional space if needed)	(b)(3) 10 USC 130e (USACE)
Recommended Change: (add additional space if needed)	

Revised

Comment Number:	3
Page Number:	Pg i and other locations throughout the report
Line Number:	Lines 19-20 and other locations throughout the report
Comment Type: A: Administrative or S: Substantive	S: Substantive
Comment: (add additional space if needed)	(b)(3) 10 USC 130e (USACE)
Recommended Change: (add additional space if needed)	

Revised

2

**Final Report
Reference**

Comment Number:	4
Page Number:	Pg i and other locations throughout the report
Line Number:	Lines 20-21 and other locations throughout the report
Comment Type: A: Administrative or S: Substantive	S: Substantive
Comment: (add additional space if needed)	(b)(3) 10 USC 130e (USACE)
Recommended Change: (add additional space if needed)	

Revised

Comment Number:	5
Page Number:	Pg i and other locations throughout the report
Line Number:	Lines 17-21, Lines 6-8 and other locations throughout the report
Comment Type: A: Administrative or S: Substantive	S: Substantive
Comment: (add additional space if needed)	(b)(3) 10 USC 130e (USACE)
Recommended Change: (add additional space if needed)	

Revised

Comment Number:	6
Page Number:	Pg i, Pg 6 and other locations throughout the report
Line Number:	Pg i, Lines 24-25, Pg 6, Lines 8-11 and other locations throughout the report
Comment Type: A: Administrative or S: Substantive	S: Substantive
Comment:	Prioritization, or ranking in order of importance, of Project security

Pages 7, 12, and 13

3

**Final Report
Reference**

(add additional space if needed)	requirements is established in accordance with (LAW) yearly updates to Engineering Circular (EC) 11-2-202, "Army Programs; Corps of Engineers Civil Works Direct Program: Program Development Guidance Fiscal Year ##### (insert Fiscal Year (FY) here)". Review of this document reveals that security items, in general terms and depending on the business line the Project is associated with, have to be ranked relatively lower than other Project requirements seeking funds from the limited Operation and Maintenance (O&M) budget. An example of this includes security being designated last priority in Increment 1 for the Flood Risk Management business line. So it may not be that the Commander's and District Engineers, Operation Project Managers (OPMs) or security manager's have placed security items lower in priority, but the EC dictates such.
Recommended Change: (add additional space if needed)	(b)(3) 10 USC 130e (USACE)

Comment Number:	7
Page Number:	Pg ii and other locations throughout the report
Line Number:	Lines 18-24 and other locations throughout the report
Comment Type: A: Administrative or S: Substantive	S: Substantive
Comment: (add additional space if needed)	(b)(3) 10 USC 130e (USACE)
Recommended Change:	

Revised

4

**Final Report
Reference**

(add additional space if needed)	(b)(3) 10 USC 130e (USACE)
----------------------------------	----------------------------

Comment Number:	8
Page Number:	Pg 3 and Pg 4
Line Number:	Pg 3, Lines 19-23, and Pg 4, Lines 1 thru 5
Comment Type: A: Administrative or S: Substantive	S: Substantive
Comment: (add additional space if needed)	(b)(3) 10 USC 130e (USACE)
Recommended Change: (add additional space if needed)	

Comment Number:	9
Page Number:	4 and other locations throughout the report
Line Number:	5 and other locations throughout the report
Comment Type: A: Administrative or	S: Substantive

Pages 3-5

Revised

Pages 3-5

5

Final Report
Reference

S: Substantive	
Comment: (add additional space if needed)	(b)(3) 10 USC 130e (USACE)
Recommended Change: (add additional space if needed)	

Revised

~~FOR OFFICIAL USE ONLY~~

CENWD Response to the DoDIG Draft Report
“USACE, Civil Works, Critical Infrastructure and Industrial Control
Systems in the Northwestern Division Were Not Always Protected”
Project No. D2012-D000LC-0080.000
September 26, 2012

The Northwestern Division has reviewed the Draft DoD IG Audit report and offers the following management comments in accordance with the Recommendation Table on page iii of the report. For the record, the nature, tone, and language of portions of this report lead the reader to ponder whether it documents an inspection or an investigation. As its stated purpose is the former, pointing out shortfalls so they can be resolved is what one would expect as the limit of its findings. Recommendations to review personnel performance and consider corrective action (B.8) against personnel seem to overstep the bounds of this activity.

Report Overall

Management Comments:

1. (b)(3) 10 USC 130e (USACE)

2.

3.

4.

Revised

Revised

~~FOR OFFICIAL USE ONLY~~

Findings

A. Critical Infrastructure in the Northwestern Division Was Not Sufficiently Protected

Recommendations

A.1 (b)(3) 10 USC 130e (USACE)

(b)(3) 10 USC 130e (USACE)

a) (b)(3) 10 USC 130e (USACE)

b)

c)

d)

Revised

Revised

Management Comments:

A.1.a. (b)(3) 10 USC 130e (USACE)


(b)(3) 10 USC 130e (USACE)

A.1.c. (b)(3) 10 USC 130e (USACE)

(b)(3) 10 USC 130e (USACE)

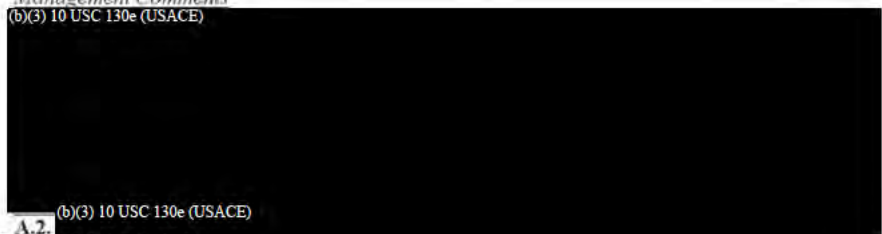
~~FOR OFFICIAL USE ONLY~~

(b)(3) 10 USC 130e (USACE)

A large rectangular area of the document is completely redacted with a solid black fill.

Management Comments


(b)(3) 10 USC 130e (USACE)

A large rectangular area of the document is completely redacted with a solid black fill.

A.2


(b)(3) 10 USC 130e (USACE)

(b)(3) 10 USC 130e (USACE)

A large rectangular area of the document is completely redacted with a solid black fill.

A.2. Management Comments:

(b)(3) 10 USC 130e (USACE)

A large rectangular area of the document is completely redacted with a solid black fill.

(b)(3) 10 USC 130e (USACE)

A rectangular area of the document is completely redacted with a solid black fill.

~~FOR OFFICIAL USE ONLY~~

A.3. (b)(3) 10 USC 130e (USACE)
(b)(3) 10 USC 130e (USACE)

A large black rectangular redaction box covering the majority of the text in section A.3.

Revised


A.3. Management Comments:

Background
(b)(3) 10 USC 130e (USACE)

A large black rectangular redaction box covering the majority of the text in the Background section.

~~FOR OFFICIAL USE ONLY~~

(b)(3) 10 USC 130e (USACE)




Management Comments

(b)(3) 10 USC 130e (USACE)




A.4 (b)(3) 10 USC 130e (USACE)
(b)(3) 10 USC 130e (USACE)




A.4. Management Comments:

A.4a. (b)(3) 10 USC 130e (USACE)


(b)(3) 10 USC 130e (USACE)



A.4b. (b)(3) 10 USC 130e (USACE)




A.5 (b)(3) 10 USC 130e (USACE)



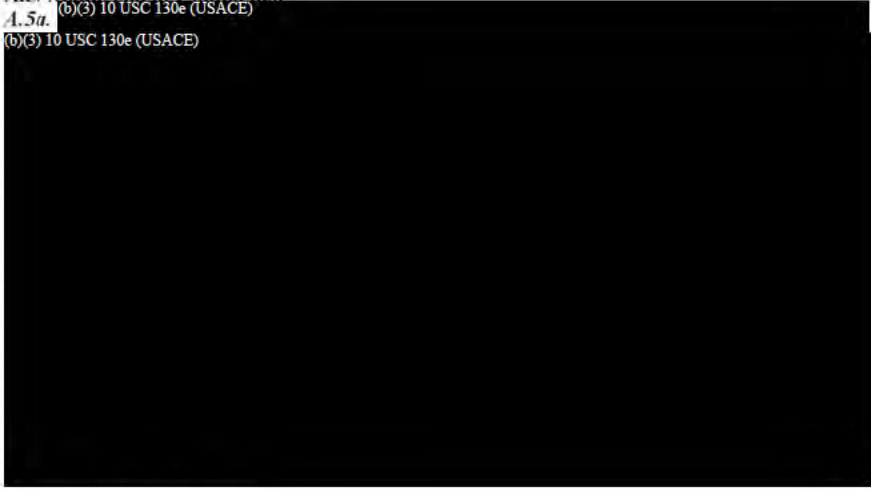
~~FOR OFFICIAL USE ONLY~~

b) (b)(3) 10 USC 130e (USACE)



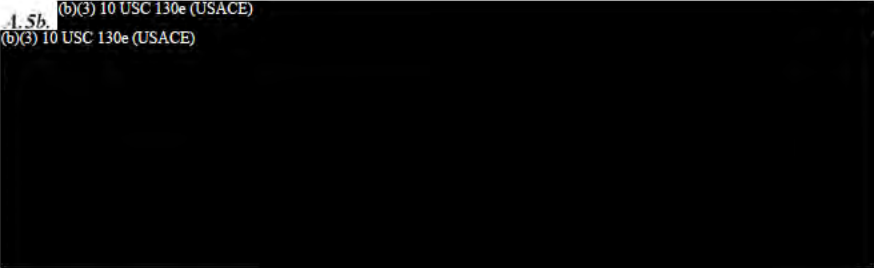
A.5. Management Comments:

A.5a. (b)(3) 10 USC 130e (USACE)




(b)(3) 10 USC 130e (USACE)

A.5b. (b)(3) 10 USC 130e (USACE)



(b)(3) 10 USC 130e (USACE)

A.6 (b)(3) 10 USC 130e (USACE)




(b)(3) 10 USC 130e (USACE)

Revised

~~FOR OFFICIAL USE ONLY~~

(b)(3) 10 USC 130e (USACE)




Revised

Deleted

Revised


A.6. Management Comments:

A.6a.1 thru 3. (b)(3) 10 USC 130e (USACE)



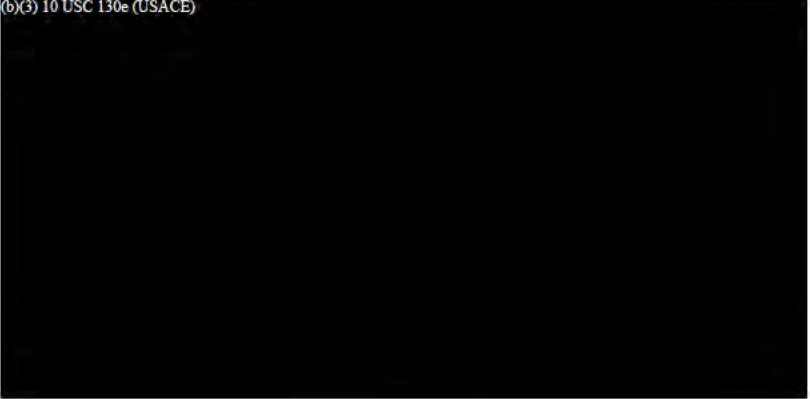
(b)(3) 10 USC 130e (USACE)

A.6a.4. (b)(3) 10 USC 130e (USACE)




(b)(3) 10 USC 130e (USACE)

A.6b. (b)(3) 10 USC 130e (USACE)



~~FOR OFFICIAL USE ONLY~~

(b)(3) 10 USC 130e (USACE)



B. Systems Used to Operate Critical Infrastructure in the Northwestern Division Were Not Always Protected Against Cyber Threats

Recommendations

B.1. We recommend that the Headquarters, U.S. Army Corps of Engineers, Programs Division, revise the current budget process to separately identify information assurance requirements to ensure sufficient funding is available to protect the industrial control systems used to operate critical infrastructure from cyber security risks.


B.1. Management Comments:

USACE HQ Response, no comment from NWD, CENWP or CENWS Required

B.2. We recommend the Chief, Hydroelectric Design Center, in coordination with the Generic Data Acquisition Control System Maintenance Team:

~~FOR OFFICIAL USE ONLY~~

(b)(3) 10 USC 130e (USACE)




Revised

Revised


B.2. Management Comments:

B.2.a (b)(3) 10 USC 130e (USACE)




(b)(3) 10 USC 130e (USACE)

~~(b)(3) 10 USC 130e (USACE)~~ (b)(3) 10 USC 130e (USACE)




(b)(3) 10 USC 130e (USACE)

B.2.b (b)(3) 10 USC 130e (USACE)




(b)(3) 10 USC 130e (USACE)

~~(b)(3) 10 USC 130e (USACE)~~ (b)(3) 10 USC 130e (USACE)



(b)(3) 10 USC 130e (USACE)


B.2.c (b)(3) 10 USC 130e (USACE)



(b)(3) 10 USC 130e (USACE)

~~FOR OFFICIAL USE ONLY~~


(b)(3) 10 USC 130e (USACE)



(b)(3) 10 USC 130e (USACE)
(b)(3) 10 USC 130e (USACE)



(b)(3) 10 USC 130e (USACE)
(b)(3) 10 USC 130e (USACE)




B3 (b)(3) 10 USC 130e (USACE)
(b)(3) 10 USC 130e (USACE)




~~FOR OFFICIAL USE ONLY~~

(b)(3) 10 USC 130e (USACE)



B.3. Management Comments:

B.3a. thru c. (b)(3) 10 USC 130e (USACE)
(b)(3) 10 USC 130e (USACE)



B.4. (b)(3) 10 USC 130e (USACE)
(b)(3) 10 USC 130e (USACE)



Final Report
Reference

~~FOR OFFICIAL USE ONLY~~

B.4. Management Comments:

~~(FOUO)~~ B.4.a (b)(3) 10 USC 130e (USACE)
(b)(3) 10 USC 130e (USACE)

~~(FOUO)~~ B.4.b (b)(3) 10 USC 130e (USACE)
(b)(3) 10 USC 130e (USACE)

~~(FOUO)~~ B.4.c (b)(3) 10 USC 130e (USACE)
(b)(3) 10 USC 130e (USACE)

B.5. (b)(3) 10 USC 130e (USACE)
(b)(3) 10 USC 130e (USACE)

B.5. Management Comments:
~~(FOUO)~~ (b)(3) 10 USC 130e (USACE)
(b)(3) 10 USC 130e (USACE)

B.6 (b)(3) 10 USC 130e (USACE)
(b)(3) 10 USC 130e (USACE)

B.6. Management Comments:
~~(FOUO)~~ (b)(3) 10 USC 130e (USACE)


B.7. We recommend that the Commander and District Engineer, Seattle District, in coordination with the Operations Project Manager for (b)(3) 10 USC 130e (USACE)

Updated Comments
Provided, Page 114

Updated Comments
Provided,
Pages 114-115

~~FOR OFFICIAL USE ONLY~~

(b)(3) 10 USC 130e (USACE)




B.7. Management Comments:

(b)(3) 10 USC 130e (USACE)

B.7a.


(b)(3) 10 USC 130e (USACE)



B.7b.

(b)(3) 10 USC 130e (USACE)


(b)(3) 10 USC 130e (USACE)



B.8.

(b)(3) 10 USC 130e (USACE)


(b)(3) 10 USC 130e (USACE)



B.8. Management Comments:

(b)(3) 10 USC 130e (USACE)

(b)(3) 10 USC 130e (USACE)




C. ICSs Were Not Properly Managed to Limit Cyber Security Risks

Recommendation:

~~FOR OFFICIAL USE ONLY~~


~~FOR OFFICIAL USE ONLY~~

(b)(3) 10 USC 130e (USACE)



C. Management Comments:

(b)(3) 10 USC 130e (USACE)



~~FOR OFFICIAL USE ONLY~~

~~FOR OFFICIAL USE ONLY~~

CENWP Responses to the DoD IG Draft Report
"USACE, Civil Works, Critical Infrastructure and Industrial Control
Systems in the Northwestern Division Were Not Always Protected"
Project No. D2012-D000LC-0080.000
September 26, 2012

The Portland District has reviewed the Draft DoD IG Audit report and offers the following updated management comments as requested by the DoD IG team.

Findings

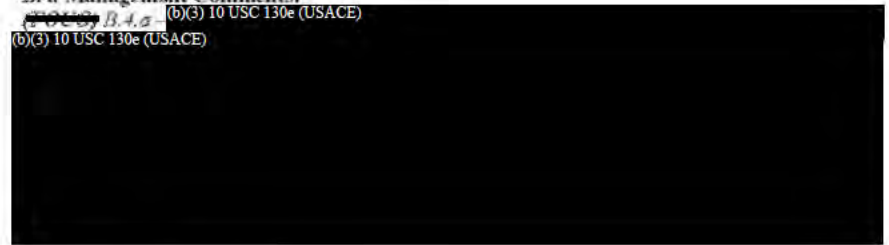
B. Systems Used to Operate Critical Infrastructure in the Northwestern Division Were Not Always Protected Against Cyber Threats

Recommendations

B.4 (b)(3) 10 USC 130e (USACE)
(b)(3) 10 USC 130e (USACE)



B.4. Management Comments:
(b)(3) 10 USC 130e (USACE)
(b)(3) 10 USC 130e (USACE)




B.6 (b)(3) 10 USC 130e (USACE)
(b)(3) 10 USC 130e (USACE)



~~FOR OFFICIAL USE ONLY~~

~~FOR OFFICIAL USE ONLY~~

(b)(3) 10 USC 130e (USACE)

A solid black rectangular redaction box covering several lines of text.

B.6. Management Comments:

~~(b)(3) 10 USC 130e (USACE)~~
(b)(3) 10 USC 130e (USACE)

A large solid black rectangular redaction box covering the majority of the page content below the 'B.6. Management Comments:' header.

~~FOR OFFICIAL USE ONLY~~

~~FOR OFFICIAL USE ONLY~~



Inspector General
Department of Defense

~~FOR OFFICIAL USE ONLY~~