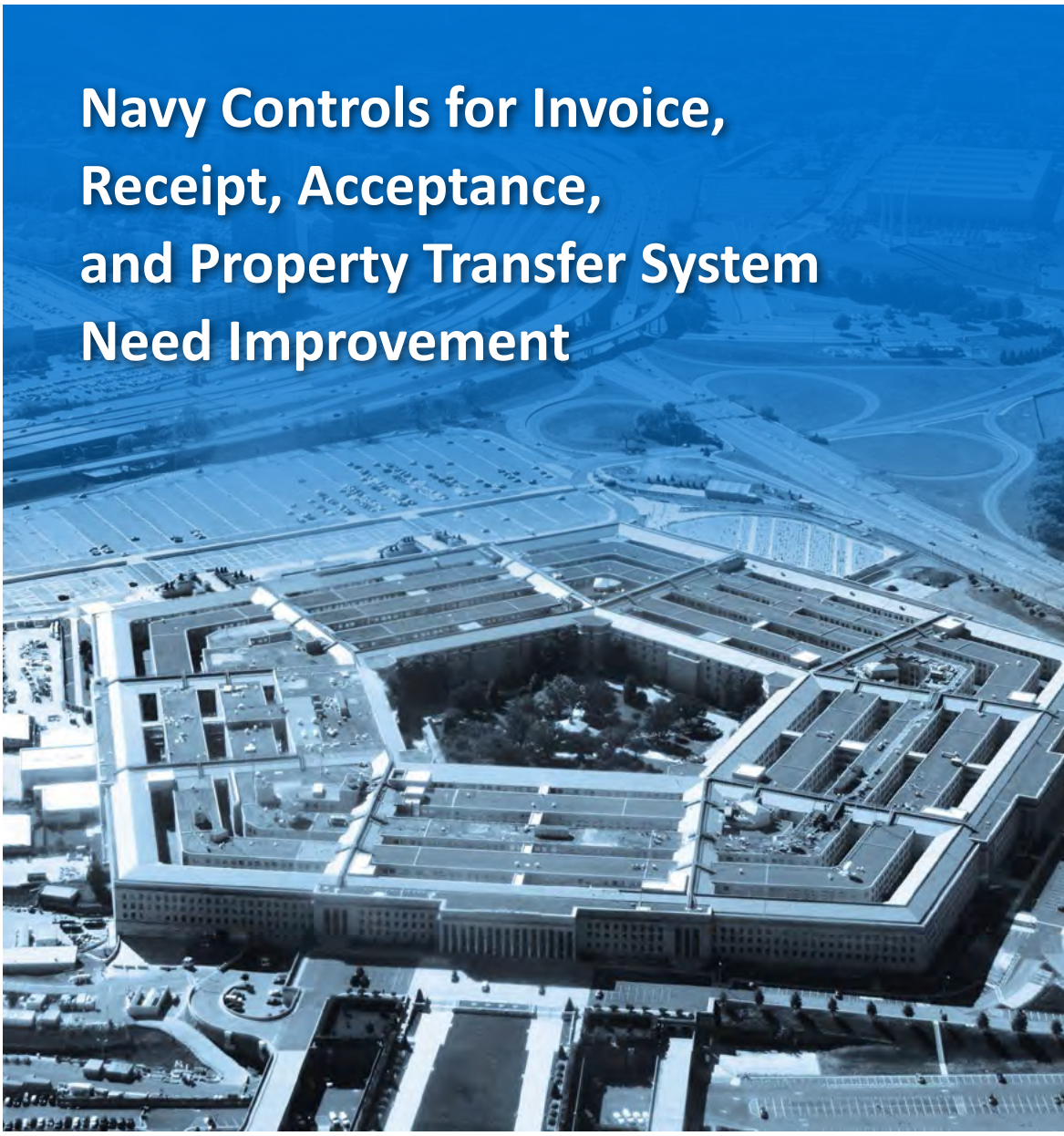
Report No. DODIG-2016-054

INSPECTOR GENERAL

U.S. Department of Defense

FEBRUARY 25, 2016

Navy Controls for Invoice, Receipt, Acceptance, and Property Transfer System Need Improvement



INTEGRITY ★ EFFICIENCY ★ ACCOUNTABILITY ★ EXCELLENCE

INTEGRITY ★ EFFICIENCY ★ ACCOUNTABILITY ★ EXCELLENCE

Mission

Our mission is to provide independent, relevant, and timely oversight of the Department of Defense that supports the warfighter; promotes accountability, integrity, and efficiency; advises the Secretary of Defense and Congress; and informs the public.

Vision

Our vision is to be a model oversight organization in the Federal Government by leading change, speaking truth, and promoting excellence—a diverse organization, working together as one professional team, recognized as leaders in our field.

Fraud, Waste & Abuse
HOTLINE
Department of Defense
dodig.mil/hotline | 800.424.9098

For more information about whistleblower protection, please see the inside back cover.

Results in Brief

Navy Controls for Invoice, Receipt, Acceptance, and Property Transfer System Need Improvement

February 25, 2016

Objective

We determined whether the Invoice, Receipt, Acceptance, and Property Transfer (iRAPT) system (formerly called wide area workflow) user organization controls administered by the Department of the Navy were designed and operating effectively. We also determined the effect of any identified deficiencies on audit readiness goals.

Finding

The iRAPT controls administered by the Navy, also referred to as complementary user entity controls (CUECs), were not designed or operating effectively for the three commands reviewed. Specifically, Navy system management did not design CUECs because they relied on the Defense Logistics Agency's controls and did not know they were required to independently develop and document CUECs. Additionally, group administrators at the three commands did not disable iRAPT accounts for separated users because Navy system management did not develop procedures for out processing, or group administrators did not make user account reviews a priority. Also, supervisors and group administrators granted certifying officers access without the proper appointment and training because they did not review appointment documents. Further, supervisors and group administrators granted users more access than required to do their job duties because they created a work around to reject misrouted invoices.

Navy system management did not develop and document change management roles, responsibilities, and procedures because they did not consider them to be significant enough to warrant documenting.

Visit us at www.dodig.mil

Finding (cont'd)

Navy Enterprise Resource Planning management did not correct a control deficiency with data sent from iRAPT to the Navy Enterprise Resource Planning system because of resource constraints.

As a result, the Navy increased the risk of unauthorized system access and improper or fraudulent payments. Undetected errors and fraud could lead to misstatements on financial statements, specifically for contractor and vendor pay, which is material to the outlays (disbursements) line on the Schedule of Budgetary Activity. Without correcting these CUECs it could impact the audit readiness goals of the Navy.

Recommendations

The Deputy Assistant Secretary of the Navy for Financial Operations should coordinate with other key stakeholders in the Navy to develop procedures to: define CUECs that clearly describe roles and responsibilities; add iRAPT users to command out-processing procedures; and review certifying officers' appointment records and training certificates. The Deputy Assistant Secretary of the Navy for Financial Operations should also review iRAPT to ensure separated employees user accounts were disabled; review training and DD Forms 577 for certifying officers at all Navy commands; disable the certifying officer role at other commands that use the Navy Enterprise Resource Planning system; and develop and implement a Navy Enterprise Resource Planning System change request. The iRAPT Program Manager at the Defense Logistics Agency should implement a system change that automatically disables user accounts after 30 days of inactivity.

Management Comments and Our Response

The Deputy Assistant Secretary of the Navy for Financial Operations addressed all specifics of Recommendation 1. However, we request additional comments from the iRAPT Program Manager, DLA, for Recommendation 2 by March 24, 2016. Please see the Recommendations Table on the back of this page.

Recommendations Table

Management	Recommendations Requiring Comment	No Additional Comments Required
Deputy Assistant Secretary of the Navy for Financial Operations		1.a.1., 1.a.2., 1.a.3., 1.a.4., 1.b., 1.c., 1.d., 1.e.
Invoice, Receipt, Acceptance, and Property Transfer System Program Manager, Defense Logistics Agency	2	

Please provide Management Comments by March 24, 2016.

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

February 25, 2016

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE (COMPTROLLER)/
CHIEF FINANCIAL OFFICER, DoD
DIRECTOR, DEFENSE LOGISTICS AGENCY
NAVAL INSPECTOR GENERAL

SUBJECT: Navy Controls for Invoice, Receipt, Acceptance, and Property Transfer System Need Improvement (Report No. DODIG-2016-054)

We are providing this report for your review and comment. The Navy processed over 75,000 invoices valued at $16.3 billion through iRAPT in the second quarter FY 2015. The Navy did not diligently document processes and implement access, configuration management, and output controls. Other organizations using iRAPT should read this report and confirm complementary user-entity controls are designed and operating effectively. We conducted this audit in accordance with generally accepted government auditing standards.

We considered management comments on a draft of this report when preparing the final report. DoD Instruction 7650.03 requires that recommendations be resolved promptly. Comments from the Deputy Assistant Secretary of the Navy for Financial Operations addressed all specifics of Recommendation 1.a.1., 1.a.2., 1.a.3., 1.a.4., 1.b., 1.c., 1.d., and 1.e. and conformed to the requirements of DoD Instruction 7650.03. However, we request comments from the Invoice, Receipt, Acceptance, and Property Transfer Program Manager, Defense Logistics Agency for Recommendation 2 by March 24, 2016.

Please provide comments that conform to the requirements of DoD Instruction 7650.03. Please send a PDF file containing your comments to audclev@dodig.mil. Copies of your comments must have the actual signature of the authorizing official for your organization. We cannot 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) 601-5945 (DSN 664-5945).

Lorin T. Venable

Lorin T. Venable, CPA
Assistant Inspector General
Financial Management and Reporting

Contents

Introduction

Objective

We determined whether the Invoice, Receipt, Acceptance, and Property Transfer (iRAPT)[1] (formerly wide area workflow) user organization controls[2] administered by the Department of the Navy were designed and operating effectively. We also determined the effect of any identified deficiencies on audit readiness goals. See Appendix A for the scope and methodology and prior audit coverage.

Background

DoD developed iRAPT as a web-based system to electronically invoice, receipt, and accept services and products from its contractors and vendors. The iRAPT system electronically shares documents between DoD and its contractors and vendors to eliminate redundant data entry, increase data accuracy, and reduce the risk of missing documents.

In the traditional DoD business method, three documents are required to make a payment: the contract, receiving report, and invoice. The contract is available in iRAPT through an interface with Electronic Data Access, a DoD contract document storage application. The iRAPT system allows contractors to submit and track invoices and receipt and acceptance documents over the web and allows government personnel to process those invoices in a real-time, paperless environment.

After the invoices are processed in iRAPT, the transaction data is transferred to the accounting systems used by that organization such as the Navy Enterprise Resource Planning (ERP) and Standard Accounting and Reporting System as accounts payable and outlays (disbursements). The Navy used iRAPT to process over 75,000 invoices valued at $16.3 billion in the second quarter FY 2015.

Program Management

The Defense Logistics Agency (DLA) is the iRAPT Program Management Office. DLA, as the service provider, provides the iRAPT system and many of the system controls for its DoD customers, or user-entities, to include the Navy. The Navy is required to know and manage all iRAPT controls that are not managed by DLA. The controls managed by the user-entity, in this case the Navy, are

[1] The audit was originally announced on wide area workflow. In FY 2015 DLA modified wide area workflow to include a suite of applications including the Invoice, Receipt, Acceptance, and Property Transfer and Electronic Data Access. DLA renamed the application iRAPT. We only performed this audit on the iRAPT application that includes the invoice, receipt, and acceptance functionality.

[2] The Navy user-organization controls are referred to in the report as the Complementary User Entity Controls.

commonly referred to as the Complementary User Entity Controls (CUECs). The Navy Research, Development, & Acquisition, Office of Financial Operations and the Program Executive Office for Enterprise Information Systems (Navy system management) cooperatively manage the CUECs for iRAPT.

Key Invoice, Receipt, Acceptance, and Property Transfer Users

Navy system management appoints group administrators as a key element of system security. Group administrators approve, activate and deactivate iRAPT user accounts. They are also responsible for reviewing accounts monthly to deactivate separated and inactive users. Before group administrators approve access, supervisors review access request forms to acknowledge the need for access and ensure training requirements are met. They are also responsible for reviewing accounts monthly to deactivate separated and inactive users. The key roles used to process invoices are the inspector, acceptor, and local processing officer (certifying officer):

- Inspectors determine if the service or product received by the government meets the terms of the contract.
- Acceptors determine if the invoice data submitted by the vendor is correct. Acceptors can act as inspectors and review products and services received.
- Certifying officers review invoices for validity and accuracy prior to certifying them for payment.

System Controls and Standards

Office of Management and Budget Circular No. A-123[3], "Management's Responsibility for Internal Control," requires that organizations that produce financial statements document the controls over financial reporting. Internal control also needs to be in place over information systems, which includes general and business process application controls.

General and business process application controls apply to all information systems. General controls help ensure the proper operation of information systems and include access, configuration management (also known as change management), and segregation of duties controls. Business process application controls help ensure the accuracy, completeness and confidentiality of transaction data within a system. These controls should be designed to ensure that transactions are properly authorized and processed accurately and that the data is valid and complete. Controls should be established when one system transmits financial information to another system to verify that the information sent is complete and

[3] Office of Management and Budget Circular No. A-123, "Management's Responsibility for Internal Control, section I."

accurate. General and business process application controls over information systems are interrelated; both are needed to ensure complete and accurate information processing.

In addition, the National Institute of Standards and Technology (NIST) Special Publication 800-35[4] requires organizations to document external service arrangements with formal contracts. The contract should specify both the user-entity's and the service provider's roles and responsibilities.

Prior Invoice, Receipt, Acceptance, and Property Transfer Control Audit

RMA Associates LLC conducted a Statement on Standards for Attestation Engagements 16[5] audit on iRAPT and issued a qualified opinion in November 2014. The reason for the qualified opinion was that interface control agreements were not in place with all systems that transmit data to and from iRAPT. RMA Associates LLC did not include the CUECs in its audit scope and, therefore, did not test the CUECs within the general and business application control areas. The U.S. Government Accountability Office Federal Information System Controls Audit Manual, February 2009, describes the general and business application controls that RMA Associates, LLC did not test.

- Access and segregation of duties controls provide reasonable assurance that access is restricted to authorized individuals and users do not have the ability to perform incompatible duties.
- Change management controls ensure system change proposals are reviewed and approved by user entity management and the changes are validated.
- Input controls reasonably assure that all data input is done in a controlled manner; data input into the application is complete, accurate, and valid; any incorrect information is identified, rejected, and corrected for subsequent processing; and the confidentiality of data is adequately protected.
- Processing controls address the completeness, accuracy, validity, and confidentiality of data as the data are processed within the application.
- Output controls assure that transaction data are complete, accurate, valid, and confidential for iRAPT and any systems that receive data from iRAPT, including any control totals.

See Appendix B for the detailed controls required for these CUECs.

[4] NIST Special Publication 800-35, "Guide to Information Technology Security Services," section 4.4.1, October 2003.

[5] Statement on Standards for Attestation Engagements 16 is the guidance from the American Institute of Certified Public Accountants for performing attestation engagements on service provider systems and controls. The purpose of this guidance is to obtain reasonable assurance that the service provider's controls are appropriately designed.

Review of Internal Controls

DoD Instruction 5010.40[6] requires DoD organizations to implement a comprehensive system of internal controls that provide reasonable assurance that programs are operating as intended and to evaluate the effectiveness of the controls. We identified internal control weaknesses at three Navy commands: Space and Naval Warfare Systems Center Pacific (SSC Pacific), Southwest Regional Maintenance Center Pacific Fleet (SWRMC), and Naval Facilities and Engineering Command Southwest (NAVFAC SW). Specifically, access controls did not ensure that accounts were disabled for inactive users; certifying officers did not have all the appointment documents and receive all the required training; and iRAPT users were given inappropriate access to system functions that they did not need to perform their jobs. In addition, configuration management roles, responsibilities, and procedures were not documented as required for the change management control. Further, output controls did not ensure that a system interface worked as intended. We will provide a copy of the report to the senior official responsible for internal controls in the Department of the Navy.

[6] DoD Instruction 5010.40, "Managers' Internal Control Program Procedures," May 30, 2013.

Finding

Navy Controls for Invoice, Receipt, Acceptance, and Property Transfer System Need Improvement

The iRAPT CUECs administered by the Navy were not designed or operating effectively at the three Navy Commands reviewed. Specifically, Navy system management did not design CUECs because they relied on the system owner's controls and did not know they were required to independently develop and document CUECs for Navy users.

Additionally, access, change management, and output controls were not operating effectively:

- Group administrators at the three commands did not disable accounts for users who left the organization because Navy system management did not develop procedures for out-processing users or group administrators did not make user account reviews a priority. In addition, supervisors granted certifying officials access without the proper appointment and training because they did not review appointment documents. Further, SSC Pacific supervisors and group administrators granted users more access than required to do their job duties because they created a work around to reject misrouted invoices.
- Navy system management did not develop change management procedures that defined roles and responsibilities and the approval process because they did not consider the procedures significant enough to warrant documenting.
- Navy ERP management did not correct a control deficiency with data sent from iRAPT to Navy ERP because of resource constraints.

As a result, the Navy increased the risk of unauthorized system access and improper, fraudulent, or late payments. Undetected errors and fraud could lead to misstatements on financial statements, specifically for contractor and vendor pay, which is material to the outlays (disbursements) line on the Schedule of Budgetary Activity. Without correcting these CUECs it could impact the audit readiness goals of the Navy.

Navy Complementary User Entity Controls Were Not Developed

The iRAPT CUECs administered by the Navy were not designed by Navy system management or operating effectively at SSC Pacific, SWRMC, and NAVFAC SW. According to Office of Management and Budget[7] and NIST[8] requirements, the Navy should establish the procedures and controls for using iRAPT and the roles and responsibilities of Navy as well as DLA. Navy system management; however, did not develop controls for processing contractor invoices in the iRAPT system. Rather, Navy system management officials stated that they relied on the system owner controls developed by DLA for its Navy users.

The Navy provided the high-level descriptions of the DLA system owner controls, but did not develop the control activities and procedures that should be implemented by the Navy.

The Navy provided the high-level descriptions of the DLA system owner controls, but did not develop the control activities and procedures that should be implemented by the Navy. Since procedures were not provided by Navy system management, Navy users did not follow a standard procedure. For instance, personnel responsible for accepting invoices developed different methods for accepting contractor requests for payment. The different methods increased the risk that errors could be made in iRAPT and improper payments could be made to vendors and contractors.

Navy system management officials stated that they did not know they were required by Office of Management and Budget and NIST to develop their own Navy-specific controls. Instead, the officials said that they relied on the controls developed and documented by DLA. Well-documented controls are essential to ensure financial information is complete and accurate since iRAPT is a significant system used in supporting the Navy financial statements. For example, Navy personnel reviewed or certified over 75,000 invoices valued at $16.3 billion in iRAPT, during the second quarter FY 2015. Developing Navy-specific controls would increase the likelihood that Navy users would properly process contractor and vendor payments in iRAPT. By doing so, the Navy would also have more assurance that CUECs, as well as DLA's service provider controls over financial reporting, are in place. Since these controls ensure the financial information is complete and accurate, absent controls increase the risk of errors that could

[7] Office of Management and Budget Circular No. A-123, "Management's Responsibility for Internal Control, section I."

[8] National Institute of Standards and Technology Special Publication 800-35, "Guide to Information Technology Security Services," section 4.4.1, October 2003.

lead to improper payments and inaccurate reporting. Navy system management should develop procedures for CUECs that define the controls for the contractor and vendor invoice process, which describes the roles and responsibilities of both the Navy and the service provider and provide procedures for all Navy users in iRAPT. Navy system management should also communicate the procedures to the Navy iRAPT user community.

Access Controls Were Not Designed and Operating Effectively

Navy system management did not design the CUECs to effectively monitor user access to iRAPT. Specifically, group administrators or supervisors did not:

- disable user accounts when employees left the organization;
- properly appoint certifying officers; and
- provide appropriate access to some users at SSC Pacific.

Access Was Not Consistently Disabled for Separated Users

The Navy did not design an effective control to disable iRAPT user accounts upon separation. Specifically, group administrators at the three commands reviewed did not timely disable iRAPT user accounts for four of five nonstatistically selected users who left the three Navy commands. According to the group administrator appointment letter, group administrators are required to perform reviews and disable user accounts when iRAPT users leave a command or when accounts become inactive. Additionally, NIST[9] and DoD[10] policy requires organizations to establish a designated time period to disable access to information systems for separated users and disable user accounts that have been inactive for 30 days. Group administrators stated that they had a lot of responsibilities, including activating and deactivating iRAPT accounts and, in most cases, this was not their primary workload. Although DLA was aware of the control deficiency, it did not take corrective action.

A NAVFAC SW group administrator stated that she did not disable access for separated employees because she had other duties, and the reviews of user accounts were not her first priority. SSC Pacific and SWRMC group administrators said that they did not disable iRAPT accounts for separated employees because management did not have out-processing procedures for supervisors to notify

[9] NIST Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations," Appendix F-PS, "PS-4 Personnel Termination," Revision 4, April 2013.

[10] Chairman of the Joint Chiefs of Staff Instruction 6510.01F, "Information Assurance and Support to Computer Network Defense," section 26.r, "Disabling and Deleting Accounts," October 10, 2013.

group administrators when an iRAPT user left the command. In one instance, we observed a group administrator disable a certifying officer's account although the employee had separated from SWRMC almost 3 months earlier. Group administrators informed us that there was no report they could run in iRAPT that would help them determine if users were inactive for an extended period of time, and the system did not automatically deactivate users.

The iRAPT system tracked when users access the system, but it did not have the capability to notify group administrators or automatically disable accounts that were inactive for more than 30 days. Failure to disable inactive accounts increases the risk of unauthorized access where invoices could be modified or destroyed leading to improper payments. DLA implemented a system change to automatically disable user accounts after 180 days of inactivity; and plans to reduce the number of days of inactivity to 60 days over time. We recommend DLA reduce the number of days to 30 days as required by DoD policy. In addition to the automated control, Navy system management should develop procedures for group administrators to review iRAPT accounts to ensure the automated control developed by DLA is working properly and ensure separated employees user accounts were automatically disabled. Navy system management should develop out-processing procedures for iRAPT users and supervisors to notify group administrators when an iRAPT user leaves a command so the account can be disabled.

Certifying Officers Lacked Proper Appointment and Required Training

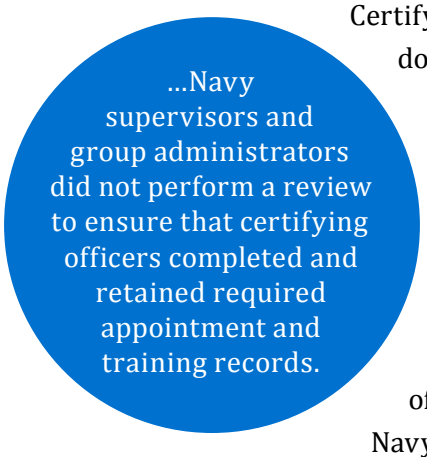
Supervisors and group administrators granted certifying officers access without proper appointment and training. The DoD FMR requires certifying officers to complete a DoD Form 577[11] to be formally appointed to certify invoices in iRAPT. The DoD FMR[12] also requires certifying officers to complete an approved Certifying Officer Legislation training course applicable to their mission area within 2 weeks of their appointment and annually thereafter. In addition, the certifying officers must provide proof of completion to their supervisor. For 5 of 28 randomly selected certifying officers:

- 2 did not maintain a DD Form 577;
- 2 did not complete the Certifying Officer Legislation training; and
- 1 did not complete a DD Form 577 or the Certifying Officer Legislation training.

[11] Department of Defense Form 577, "Appointment/Termination Record - Authorized Signature," November 2014 as required by DoD Regulation 7000.14-R, "DoD Financial Management Regulation," volume 5, chapter 5, section 050401.

[12] DoD Regulation 7000.14-R, "DoD Financial Management Regulation," volume 5, chapter 5, section 050304.

According to iRAPT records, 3 of the 5[13] certifying officers certified 469 invoices, valued at $100 million from January 1 through May 20, 2015, to vendors and contractors without the proper authority to do so. For example, two certifying officers at NAVFAC SW provided a DD Form 577 dated June 4, 2015; however, these employees performed the certifying officer role in iRAPT for at least 3 years without a proper appointment. Defense Finance and Accounting Service personnel who maintain the official DD Form 577 database for DoD stated that the DD Forms 577 for these certifying officers were not on file before June 2015.



Certifying officers did not have the required appointment documents or training because Navy supervisors and group administrators did not perform a review to ensure that certifying officers completed and retained required appointment and training records. Certifying officers are required to certify invoices and vouchers as proper for payment and that the proposed payments are legal, proper, and correct. The Navy increased the risk of improper payments from certifying officers who lack proper training and accountability. Navy system management should develop procedures for supervisors and group administrators to ensure their certifying officers prepare and retain appointment forms and complete required training with 2 weeks as required for initial appointment and annually thereafter. In addition, Navy system management should conduct a review, or direct group administrators to review training certifications and DD Forms 577 for certifying officers throughout all Navy commands.

Some Users Had Inappropriate Access to the Certifying Role

SSC Pacific group administrators authorized 1 of 28 randomly selected certifying officers more access to iRAPT than was required to perform their duties. The business process at SSC Pacific was different from the other two commands; its certifying officials did not certify invoices in iRAPT. Rather, SSC Pacific personnel certified invoices in Navy ERP and, therefore, the iRAPT certifying role was not needed for SSC Pacific employees.

During the audit, we identified two more users, and SSC Pacific personnel also identified another, for a total of four users with access to the certifying official role in iRAPT. According to NIST[14], organizations should grant users privilege levels

[13] A certifying officer from SSC Pacific and another from SWRMC were not identified as the certifying officer for any invoice in iRAPT.

[14] NIST Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations," Appendix F-AC, "AC-6 Least Privilege," Revision 4, April 2013.

no higher than what is necessary to accomplish required business functions. The group administrators stated that they granted the employees the certifying role as a work around to reject misrouted invoices sent by vendors and contractors. The administrators stated that they believed this was the best way to correct invoices submitted by vendors and contractors that were routed to SSC Pacific incorrectly. However, the certifying officer role provided all four users the unnecessary privilege to certify invoices within iRAPT. The ability to approve invoices, either purposefully or inadvertently, increased the risk of inappropriate access and improper or fraudulent payments. The four users did not certify any invoices for payment between January 1 and March 31, 2015.

During the course of the audit, a Navy Research, Development, & Acquisition official determined the certifying officer role could be disabled. She stated that doing so would force vendors to enter correct information into iRAPT, which would eliminate misrouted invoices. Since SSC Pacific group administrators took corrective action and disabled the certifying officer role for the four iRAPT users, we did not make a recommendation in this specific finding. However, other Navy commands use iRAPT and Navy ERP, which may result in using the certifying officer role to reject invoices at other commands. Navy System Management should conduct a review of other commands that use Navy ERP and determine whether the commands should disable the certifying officer role in iRAPT.

Change Management Controls Were Not Designed or Operating Effectively

Navy system management did not document the roles and responsibilities or the approval process for officials involved in the iRAPT change management process. NIST[15] states that the organization should develop and document a change management policy that addresses roles, responsibilities, and coordination, as well as compliance, for all organizations involved in the process. In addition, the organization should document and retain records for change management.

According to a Navy Research, Development, and Acquisition official, system change proposals recommended by users should be reviewed and approved by the command group administrators. Once approved by the command's group administrator, the change proposal is forwarded to Navy system management-level group administrator for review and approval. Only those change proposals approved by the group administrator are forwarded to the DLA iRAPT Operational Review Committee for consideration. Initially, Navy System Management did not

[15] NIST Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations," Appendix F-CA, "CM-1 Configuration Management Policies and Procedures," Revision 4, April 2013.

provide approvals and documentation that supported this process. However, after we made multiple attempts to obtain the information, Navy System Management provided documentation to support the process and the five change proposals that we nonstatistically sampled.

Navy system management officials stated that they did not develop change management procedures because they did not consider them to be significant enough to document. By not having a documented process for change management, Navy increased the risk of unapproved system changes. During the audit, Navy system management officials defined and documented their CUECs for change management for iRAPT. These CUECs defined roles and responsibilities that included a documented process to request, review, and approve system change proposals for the iRAPT system. By documenting the change management procedures, Navy system management decreases the risk of unapproved system changes that could compromise the Navy's invoice, receipt, and acceptance business process. Since Navy system management took corrective action, we did not make a recommendation to this specific finding.

An Output Control Did Not Operate Effectively at Space and Naval Warfare Systems Center Pacific

Navy ERP Program Management Office did not develop an effective output control for data transmitted between iRAPT and Navy ERP. The iRAPT system transmitted invoice data to Navy ERP for certification; however, Navy ERP did not always accept the invoice data from iRAPT, which resulted in lost data. SSC Pacific pay personnel stated invoice data did not transfer properly from iRAPT to Navy ERP when acceptance of goods or services was initiated in Navy ERP. SSC Pacific pay personnel were required to manually review the invoices to validate that the invoice information was accurate and complete. In addition, SSC Pacific pay personnel responsible for processing vendor and contractor invoices stated that iRAPT could not identify how many invoices were transmitted from iRAPT to Navy ERP. Instead, the differences between the number of invoices iRAPT transmitted and the number received by Navy ERP had to be manually reviewed and reconciled by pay personnel. This invoice information is essential to ensuring that financial data sent between systems is transmitted and received properly. In addition, the manual reconciliation led to inefficient use of time and an increased risk of late payments to contractors and errors in Navy ERP.

...Navy ERP did not always accept the invoice data from iRAPT, which resulted in lost data.

Although officials from the program management office stated that they knew about the problems with data transferring from iRAPT to the Navy ERP system since FY 2012, they did not implement the required system changes due to resource constraints. According to the Navy ERP program management office the Navy ERP change proposal may not fix this problem. The iRAPT interface was scheduled to be corrected in the first quarter FY 2016. The Navy is trying to correct as many problems with Navy ERP as possible, but corrective actions have been delayed due to constrained resources. Navy System Management should develop and implement a Navy ERP system change request that will enable iRAPT to transmit complete and accurate invoice information to the Navy ERP system and eliminate the need for inefficient manual data entry and reconciliation.

Impact on Payments and Audit Readiness

Navy personnel certified over 75,000 invoices valued at $16.3 billion during the second quarter FY 2015. Without correcting the CUEC weaknesses identified in this report, the Navy increases the risk of improper or fraudulent payments, errors, and incomplete financial accounting data. There is also an increased risk that interest would be paid to contractors due to late payments. Undetected fraud and errors could lead to misstatements on the financial statements, specifically contractor and vendor pay, which is material to the outlays (disbursements) line on the Schedule of Budgetary Activity.

Recommendations, Management Comments, and Our Response

Recommendation 1

We recommend the Deputy Assistant Secretary of the Navy for Financial Operations coordinate with the Deputy Assistant Secretary of the Navy for Acquisition and Procurement and the Director of the Program Executive Office for Enterprise Information Systems to:

a. Develop and communicate comprehensive procedures to:

1. Define controls for the contractor and vendor invoice process that clearly describe the roles and responsibilities of both the Department of the Navy and the service provider, Defense Logistics Agency, and provide procedures for the Invoice, Receipt, Acceptance, and Property Transfer system users to follow at all commands.

Deputy Assistant Secretary of the Navy for Financial Operations Comments

The Deputy Assistant Secretary of the Navy for Financial Operations agreed, stating that Navy-specific controls for the contractor and vendor invoice process needs to be defined to supplement controls provided by the iRAPT system service provider, Defense Logistics Agency. The Deputy Assistant Secretary also agreed that the procedures for iRAPT system users needs to be standardized across all commands to reduce process variation and the risk of improper payments. The Office of Financial Operations will coordinate with the Deputy Assistant Secretary of the Navy for Acquisition and Procurement to define standard Navy-specific controls to supplement Defense Logistics Agency controls, as well as to standardize iRAPT procedures across all Navy commands.

2. **Out-process Invoice, Receipt, Acceptance, and Property Transfer system users who leave the commands. Both users and supervisors should provide a formal notification to the Invoice, Receipt, Acceptance, and Property Transfer system group administrator indicating that a user is separating from the command and the corresponding system access should end.**

Deputy Assistant Secretary of the Navy for Financial Operations Comments

The Deputy Assistant Secretary of the Navy for Financial Operations agreed, stating that she plans to coordinate with systems owners to correct this deficiency across the Navy by June 2016.

3. **Review the DD Forms 577 of certifying officers before giving system access to certify invoices.**
4. **Review the training of certifying officers within two weeks of appointment and annually thereafter.**

Deputy Assistant Secretary of the Navy for Financial Operations Comments

The Deputy Assistant Secretary of the Navy for Financial Operations agreed, stating that since the audit was conducted, the Assistant Secretary of the Navy (Financial Management and Comptroller) issued "Financial Management Policy Letter 16-0 1: Delegation of Authority to Appoint Accountable Officials," December, 8, 2015, to major commands. This new guidance requires that DD Forms 577 are valid before granting system access to certifying officers and that employees appointed as certifying officials complete training in accordance with DoD Regulation 7000.14-R, "DoD Financial Management Regulation," volume 5, which requires training completion within 2 weeks of appointment and annually thereafter. Office of Financial Operations personnel will further instruct Navy commands to review and update their internal guidance to ensure commands are in compliance with Financial Management Policy Letter 16-0 1.

b. Review the Invoice, Receipt, Acceptance, and Property Transfer system to verify that the Defense Logistics Agency's automated control for inactive users is working properly and ensure separated employees user accounts were automatically disabled.

Deputy Assistant Secretary of the Navy for Financial Operations Comments

The Deputy Assistant Secretary of the Navy for Financial Operations agreed, stating that she will coordinate with the Director of the Program Executive Office for Enterprise Information Systems to ensure automated controls for inactive users are working properly. If automated controls are not working properly, the Defense Logistics Agency will be notified to implement manual controls until problems with automated controls are resolved.

c. Review, or direct group administrators to review, the completion of training and DD Forms 577 for certifying officers at all Navy commands.

Deputy Assistant Secretary of the Navy for Financial Operations Comments

The Deputy Assistant Secretary of the Navy for Financial Operations agreed, stating that the Assistant Secretary of the Navy (Financial Management and Comptroller) issued "Financial Management Policy Letter 16-0 1: Delegation of Authority to Appoint Accountable Officials," December 8, 2015, to major commands regarding the completion of training and DD Forms 577 for certifying officers. Office of Financial Operations personnel will further instruct Navy commands to review and update their internal guidance and procedures to ensure commands are in compliance with Financial Management Policy Letter 16-0 1.

d. Review other commands that use the Navy Enterprise Resource Planning system and direct the commands to disable the certifying officer role in the Invoice, Receipt, Acceptance, and Property Transfer system if their duties do not require it.

Deputy Assistant Secretary of the Navy for Financial Operations Comments

The Deputy Assistant Secretary of the Navy for Financial Operations agreed, stating that commands will review all users that have certifying officer roles in the iRAPT system and disable the certifying officer roles of users who do not require certifying officer roles.

e. Develop and implement the Navy Enterprise Resource Planning system change request that will enable the Invoice, Receipt, Acceptance, and Property Transfer system to transmit information to the Navy Enterprise Resource Planning system.

Deputy Assistant Secretary of the Navy for Financial Operations Comments

The Deputy Assistant Secretary of the Navy for Financial Operations agreed, stating that a change request is currently being developed to improve the transmission of information between the iRAPT system and the Navy Enterprise Resource Planning system. Implementation is anticipated by November 2016.

Our Response

Comments from the Deputy Assistant Secretary addressed all specifics of the recommendations, and no further comments are required.

Recommendation 2

We recommend that the Invoice, Receipt, Acceptance, and Property Transfer Program Manager, Defense Logistics Agency reduce the number of days required for automatic user account deactivation to 30 days to meet DoD policy.

Invoice, Receipt, Acceptance, and Property Transfer Program Manager, Defense Logistics Agency Comments

The Invoice, Receipt, Acceptance, and Property Transfer Program Manager, Defense Logistics Agency did not provide comments that conform to requirements.

Our Response

We request the Invoice, Receipt, Acceptance, and Property Transfer Program Manager, Defense Logistics Agency provide comments to the final report.

Appendix A

Scope and Methodology

We conducted this performance audit from February 2015 through December 2015 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 limited our review to invoices, receiving reports, personnel, and CUECs in place between January 1 and March 31, 2015. We nonstatistically selected three Navy commands: SSC Pacific, SWRMC, and NAVFAC SW to review during the audit. We selected two Navy commands based on the volume and dollar amount from the top 10 Navy commands for transactions submitted and processed from January 1, 2015, through March 31, 2015. In addition, we selected SWRMC because of its close proximity to the other two commands.

To test access controls, we used the control test outlined in section 450 of the Government Accountability Office Financial Audit Manual and the sample size figure in the Journal of Public Inquiry, Fall/Winter 2012-2013[16] to select users and transactions for internal control testing. We obtained a population of users from the Navy for the three commands located in San Diego, California. We selected a simple random sample based on user attributes with a 90-percent confidence level. We selected 28 out of 57 certifying officers and 44 out of 793 users from a combination of acceptors, inspectors, and local processing officer reviewers. In addition, we selected a nonstatistical sample of 5 out of 7separated employees and reviewed all 14 group administrators. We tested:

- user access authorization;
- physical access to workstations or other computer devices used to access the iRAPT system;
- segregation of duties; and
- iRAPT system access privileges.

We requested documentation to support the user roles and responsibilities. In addition, we observed iRAPT users accept and certify invoices. We also interviewed iRAPT users at each level of the approval process to determine their understanding of the roles and responsibilities.

[16] Journal of Public Inquiry, Fall/Winter 2012-2013, "Statistical Sampling: Choosing the Right Sample Size," Figure 3: The Population and the Sample Size for Internal Control Test, Dr. Kandasamy Selvavel and James Hartman Jr.

To test change management controls, we reviewed the last five iRAPT system change proposals from within the Navy user community to determine if complementary user controls included a documented process to request, review, and approve system change proposals for iRAPT.

Navy system management did not document the input, processing, and output controls. Therefore, we could not determine what management considered to be their controls for these areas. Rather than test documented controls, we tested the accuracy and completeness of the transactions processed in iRAPT. We obtained a population of transactions for goods shipped to and services performed in San Diego, California, from January 1, 2015, through March 31, 2015, for the three Navy commands. Since both NAVFAC SW and SWRMC used the Standard Accounting and Reporting System, we selected a random sample of 45 transactions, valued at $5.7 million from a population of 3,802 transactions, valued at $485 million. Since SSC Pacific used the Navy ERP system, we selected a random sample of 44 transactions, valued at $5 million from a population of 515 transactions, valued at $46.6 million.

Our testing of the 89 invoices found that all were accurate and processed by the commands within required timeframes. We also discussed interface control agreements between iRAPT and the various entitlement systems and a memorandum of understanding between Navy and the Defense Finance and Accounting Service to ensure there were agreements and memorandums in place and adequate.

We met with key personnel from the Offices of the Deputy Assistant Secretary of the Navy; Financial Operations and Acquisition and Procurement, Program Executive Office for Enterprise Information Systems; SSC Pacific, SWRMC, NAVFAC SW, DLA; and Defense Finance and Accounting Service to identify policies and procedures in place over the access, configuration management, input, processing, and output controls of processing invoices in iRAPT.

Using iRAPT's functional auditor role, we reviewed the supporting documents for the sampled invoice transactions including contracts, invoices, and receiving reports. We also reviewed applicable Office of Management and Budget, NIST, DoD and Navy policies and procedures such as volume 5, chapter 5 of the DoD FMR to determine established requirements.

Use of Computer-Processed Data

We used computer-processed data extracted from iRAPT to perform our audit. DLA personnel extracted invoice and user account data from iRAPT for the three commands reviewed and compiled into Excel spreadsheets. To test data reliability, we reviewed information about iRAPT such as the Statement on Standards for Attestation Engagements 16 report, Navy ERP iRAPT system controls, obtained corroborating evidence, and traced the sample item data to its source documents. Further, we cross-checked data for each sample item to the corresponding source documents. As a result, we determined the data were sufficiently reliable for the purposes of this report.

Use of Technical Assistance

Statisticians from Office of the Deputy Inspector General Quantitative Methods Division developed our statistical samples of iRAPT users and invoice transactions and provided guidance for selecting nonstatistical samples.

Prior Coverage

During the last 5 years, the Department of Defense Inspector General issued one report on the Navy Office of Financial Operations and lack of a system interface between the Navy ERP system and iRAPT to ensure liability recognition was performed in a timely manner. Unrestricted DoD IG reports can be found at http://www.dodig.mil/pubs/index.cfm.

DoD IG

Report No. DODIG-2015-142 "Navy's Contract/Vendor Pay Process Was Not Auditable," July 1, 2015

Appendix B

Description of Complementary User-Entity Controls

We limited the scope of our audit to the CUECs that were not tested by RMA Associates LLC in the 2014 SSAE 16 audit. According to RMA Associates LLC's November 2014 opinion, the CUECs not tested for iRAPT were:

- Access Controls and Segregation of Duties
  - User entity staff receives appropriate security awareness training.
  - Logical access to the iRAPT system using computer terminals or other computer devices located at or administered by user entities is restricted to authorized user entity staff.
  - Physical access to workstations or other computer devices used to access the iRAPT system that are located at or administered by user entities is restricted to authorized user entity staff.
  - The following takes place for staff with access to user entity information systems used to access the iRAPT system:
    - A standard account request form is completed and maintained for user account creations, modifications and deletions.
    - Requests for user accounts are only submitted for those staff appropriately approved to receive application access.
    - User accounts and associated privileges are reviewed on a periodic basis to ensure they remain commensurate with job responsibilities.
    - User accounts are removed on a timely basis as appropriate.
    - User entity staff access to the iRAPT system has been duly authorized by an appropriate member of user entity management.
  - iRAPT system access privileges, when combined with each other or with privileges in other user entity-operated information systems, provide staff with the ability to perform duties considered incompatible by user entity management, are properly segregated.
  - The IRAPT Program Management Office or Electronic Business Operational Support Team are promptly notified of any required change or termination in user entity staff that possess top level group administrator access to the iRAPT system so the access can be updated or disabled in a timely manner.

- Change Management
    - Requests to modify the iRAPT system functionality submitted by the user entity to iRAPT Operational Review Committee have been reviewed and approved by user entity management.
    - User entities evaluate changes applied in each iRAPT system release and perform procedures deemed necessary through Operational Requirements Committee and Electronic Business Configuration Control discussions to validate the changed functionality or impact on other related functionalities within the iRAPT system.
- Input
    - User entity staff is responsible for data submitted to the iRAPT system is complete, accurate, timely and appropriately authorized.
    - User entity staff is responsible for verifying vendors are in compliance with the policies and procedures for submitting item unique identification and radio-frequency identification information specified in their contracts.
- Processing
    - Data processed by the IRAPT system is complete, accurate, timely, and appropriately authorized by user entity staff.
    - User entity staff monitors the receipt of expected transactions and reports to determine whether they are delivered in a timely manner and, if they are not, promptly informs the Defense Information Systems Agency through the help desk or ticketing system.
    - User entity staff reviews error messages displayed during processing and follows up on exceptions in an authorized, complete, accurate, and timely manner.
- Output
    - User entity staff reviews output provided by the iRAPT system to ensure completeness, accuracy, and timeliness.

Management Comments

Deputy Assistant Secretary of the Navy Comments

DEPARTMENT OF THE NAVY
OFFICE OF THE ASSISTANT SECRETARY
(FINANCIAL MANAGEMENT AND COMPTROLLER)
1000 NAVY PENTAGON
WASHINGTON, DC 20350-1000

JAN 22 2016

MEMORANDUM FOR DEPARTMENT OF DEFENSE INSPECTOR GENERAL

SUBJECT: Response to DoDIG Draft Report D2015-D000FS-0120.000 "Navy Controls for Invoice, Receipt, Acceptance, and Property Transfer System Need Improvement", December 24, 2015

In accordance with the reference, the Department of the Navy has reviewed the subject draft report and provided the following comments in the attachments.

If you have any questions or concerns my point of contact for this matter is [redacted]

Karen L. Fenstermacher

Karen L. Fenstermacher
Deputy Assistant Secretary of the Navy
(Financial Operations)

Attachments:
As stated

Deputy Assistant Secretary of the Navy Comments (cont'd)

DODIG DRAFT REPORT D2015-D000FS-0120.000
DECEMBER 24, 2015

"NAVY CONTROLS FOR INVOICE, RECEIPT, ACCEPTANCE, AND PROPERTY TRANSFER SYSTEM NEED IMPROVEMENT"

DEPARTMENT OF THE ANVY COMMENTS TO THE DODIG DRAFT REPORT D2015-D000FS-0120.000

PAGE 12, RECOMMENDATIONS, RECOMMENDATION 1.A.1:

"DEFINE CONTROLS FOR THE CONTRACTOR AND VENDOR INVOICE PROCESS THAT CLEARLY DESCRIBE THE ROLES AND RESPONSIBILITIES OF BOTH THE DEPARTMENT OF THE NAVY AND THE SERVICE PROVIDER AND PROVIDE PROCEDURES FOR THE INVOICE, RECEIPT, ACCEPTANCE, AND PROPERTY TRANSFER SYSTEM USERS TO FOLLOW AT ALL COMMANDS."

COMMENT:

CONCUR. TO AVOID POTENTIAL CONFUSION, WE REQUEST CLARIFICATION IN THE WORDING OF THE RECOMMENDATION REGARDING WHETHER THE TERM "SERVICE PROVIDER" IN THIS RECOMMENDATION REFERS TO "SERVICE PROVIDER" OF THE IRAPT SYSTEM, WHICH IS THE DEFENSE LOGISTICS AGENCY (DLA); OR THE "SERVICE PROVIDER" OF GOODS AND SERVICES TO THE NAVY, WHICH IS THE VENDOR. THIS COMMENT IS WRITTEN WITH THE "SERVICE PROVIDER" BEING THE DLA.

THE NAVY OFFICE OF FINANCIAL OPERATIONS (FMO) CONCURS THAT NAVY-SPECIFIC CONTROLS FOR THE CONTRACTOR AND VENDOR INVOICE PROCESS NEEDS TO BE DEFINED TO SUPPLEMENT CONTROLS PROVIDED BY THE IRAPT SYSTEM SERVICE PROVIDER, THE DEFENSE LOGISTICS AGENCY (DLA). FMO ALSO CONCURS THAT THE PROCEDURES FOR IRAPT SYSTEM USERS NEEDS TO BE STANDARDIZED ACROSS ALL COMMANDS TO REDUCE PROCESS VARIATION AND REDUCE THE RISK OF IMPROPER PAYMENTS; HOWEVER, FMO IS NOT THE LEAD FOR ACQUISITION FUNCTIONS INCLUDING INVOICE, RECEIPT, AND ACCEPTANCE. FMO WILL COORDINATE WITH THE DEPUTY ASSISTANT SECRETARY OF THE NAVY FOR ACQUISITION AND PROCUREMENT (DASN (AP)) TO DEFINE STANDARD NAVY-SPECIFIC CONTROLS TO SUPPLEMENT DLA CONTROLS, AS WELL AS TO STANDARDIZE IRAPT PROCEDURES ACROSS ALL NAVY COMMANDS.

PAGE 13, RECOMMENDATIONS, RECOMMENDATION 1.A.2:

"OUT-PROCESS INVOICE, RECEIPT, ACCEPTANCE, AND PROPERTY TRANSFER SYSTEM USERS WHO LEAVE THE COMMANDS. BOTH USERS AND SUPERVISORS SHOULD PROVIDE A FORMAL NOTIFICATION TO THE INVOICE, RECEIPT, ACCEPTANCE, AND PROPERTY TRANSFER SYSTEM GROUP ADMINISTRATOR INDICATING THAT A USER IS SEPARATING FROM THE COMMAND AND THE CORRESPONDING SYSTEM ACCESS SHOULD END."

COMMENT:

CONCUR. THE NAVY OFFICE OF FINANCIAL OPERATIONS (FMO) RECEIVED NOTIFICATION OF FINDINGS AND RECOMMENDATIONS (NRFS) REFLECTING THESE DEFICIENCIES ACROSS THE INFORMATION TECHNOLOGY PORTFOLIO. FMO, IN COORDINATION WITH SYSTEM OWNERS, IS WORKING TO REMEDIATE THESE DEFICIENCIES, AND ANTICIPATES COMPLETION NO LATER THAN JUNE 2016.

Deputy Assistant Secretary of the Navy Comments (cont'd)

PAGE 13, RECOMMENDATIONS, RECOMMENDATION 1.A.3:

"REVIEW THE DD FORMS 577 OF CERTIFYING OFFICERS BEFORE GIVING SYSTEM ACCESS TO CERTIFY INVOICES."

COMMENT:

CONCUR. SINCE THE DOD IG REVIEW WAS CONDUCTED, THE ASSISTANT SECRETARY OF THE NAVY (FINANCIAL MANAGEMENT AND COMPTROLLER) HAS ISSUED REFERENCE (A) "FINANCIAL MANAGEMENT POLICY LETTER 16-0 1: DELEGATION OF AUTHORITY TO APPOINT ACCOUNTABLE OFFICIALS" TO MAJOR COMMANDS ENSURING THAT DD FORMS 577 ARE VALID PRIOR TO GRANTING SYSTEM ACCESS TO CERTIFYING OFFICERS.

PAGE 13, RECOMMENDATIONS, RECOMMENDATION 1.A.4:

"REVIEW THE TRAINING OF CERTIFYING OFFICERS WITHIN TWO WEEKS OF APPOINTMENT AND ANNUALLY THEREAFTER."

COMMENT:

CONCUR. SINCE THE DOD IG REVIEW WAS CONDUCTED, THE ASSISTANT SECRETARY OF THE NAVY (FINANCIAL MANAGEMENT AND COMPTROLLER) HAS ISSUED REFERENCE (A) "FINANCIAL MANAGEMENT POLICY LETTER 16-0 1: DELEGATION OF AUTHORITY TO APPOINT ACCOUNTABLE OFFICIALS" TO MAJOR COMMANDS ENSURING THAT EMPLOYEES APPOINTED AS CERTIFYING OFFICERS COMPLETE TRAINING IN ACCORDANCE WITH THE DOD FINANCIAL MANAGEMENT REGULATION (FMR) 7000.14-R, VOL. 5, WHICH REQUIRES TRAINING COMPLETION WITHIN TWO WEEKS OF APPOINTMENT AND ANNUALLY THEREAFTER. THE NAVY OFFICE OF FINANCIAL OPERATIONS (FMO) WILL FURTHER INSTRUCT NAVY COMMANDS TO REVIEW AND UPDATE THEIR INTERNAL GUIDANCE TO ENSURE COMMANDS ARE IN COMPLIANCE WITH FINANCIAL MANAGEMENT POLICY LETTER 16-0 1.

PAGE 13, RECOMMENDATIONS, RECOMMENDATION 1.B:

"REVIEW THE INVOICE, RECEIPT, ACCEPTANCE, AND PROPERTY TRANSFER SYSTEM TO VERIFY THAT THE DEFENSE LOGISTICS AGENCY'S AUTOMATED CONTROL FOR INACTIVE USERS IS WORKING PROPERLY AND ENSURE SEPARATED EMPLOYEES USER ACCOUNTS WERE AUTOMATICALLY DISABLED."

COMMENT:

CONCUR. THE NAVY OFFICE OF FINANCIAL OPERATIONS (FMO) WILL COORDINATE WITH THE DIRECTOR OF THE PROGRAM EXECUTIVE OFFICE FOR ENTERPRISE INFORMATION SYSTEMS (PEO EIS) TO ENSURE AUTOMATED CONTROLS FOR INACTIVE USERS ARE WORKING PROPERLY. IF AUTOMATED CONTROLS ARE NOT WORKING PROPERLY, THEY WILL BE BROUGHT TO THE ATTENTION OF THE DEFENSE LOGISTICS AGENCY (DLA), AND MANUAL CONTROLS WILL BE IMPLEMENTED IN THEIR PLACE UNTIL PROBLEMS WITH AUTOMATED CONTROLS ARE RESOLVED.

2

Deputy Assistant Secretary of the Navy Comments (cont'd)

PAGE 13, RECOMMENDATIONS, RECOMMENDATION 1.C:

"REVIEW, OR DIRECT GROUP ADMINISTRATORS TO REVIEW, THE COMPLETION OF TRAINING AND DD FORMS 577 FOR CERTIFYING OFFICERS AT ALL NAVY COMMANDS."

COMMENT:

CONCUR. SINCE THE DOD IG REVIEW WAS CONDUCTED, THE ASSISTANT SECRETARY OF THE NAVY (FINANCIAL MANAGEMENT AND COMPTROLLER) HAS ISSUED REFERENCE (A) "FINANCIAL MANAGEMENT POLICY LETTER 16-0 1: DELEGATION OF AUTHORITY TO APPOINT ACCOUNTABLE OFFICIALS" TO MAJOR COMMANDS REGARDING THE COMPLETION OF TRAINING AND DD FORMS 577 FOR CERTIFYING OFFICERS. THE NAVY OFFICE OF FINANCIAL OPERATIONS (FMO) WILL FURTHER INSTRUCT NAVY COMMANDS TO REVIEW AND UPDATE THEIR INTERNAL GUIDANCE AND PROCEDURES TO ENSURE COMMANDS ARE IN COMPLIANCE WITH FINANCIAL MANAGEMENT POLICY LETTER 16-0 1.

PAGE 13, RECOMMENDATIONS, RECOMMENDATION 1.D:

"REVIEW OTHER COMMANDS THAT USE THE NAVY ENTERPRISE RESOURCE PLANNING SYSTEM AND DIRECT THE COMMANDS TO DISABLE THE CERTIFYING OFFICER ROLE IN THE INVOICE, RECEIPT, ACCEPTANCE, AND PROPERTY TRANSFER SYSTEM IF THEIR DUTIES DO NOT REQUIRE IT."

COMMENT:

CONCUR. THE NAVY OFFICE OF FINANCIAL OPERATIONS (FMO) WILL ENSURE COMMANDS REVIEW ALL USERS THAT HAVE CERTIFYING OFFICER ROLES IN THE IRAPT SYSTEM, AND DISABLE THE CERTIFYING OFFICER ROLES OF USERS WHOM DO NOT REQUIRE CERTIFYING OFFICER ROLES.

PAGE 13, RECOMMENDATIONS, RECOMMENDATION 1.E:

"DEVELOP AND IMPLEMENT THE NAVY ENTERPRISE RESOURCE PLANNING SYSTEM CHANGE REQUEST THAT WILL ENABLE THE INVOICE, RECEIPT, ACCEPTANCE, AND PROPERTY TRANSFER SYSTEM TO TRANSMIT INFORMATION TO THE NAVY ENTERPRISE RESOURCE PLANNING SYSTEM."

COMMENT:

CONCUR. A CHANGE REQUEST IS CURRENTLY BEING DEVELOPED TO IMPROVE THE TRANSMISSION OF INFORMATION BETWEEN THE IRAPT SYSTEM AND THE NAVY ENTERPRISE RESOURCE PLANNING (NAVY ERP) SYSTEM. IMPLEMENTATION IS ANTICIPATED NOVEMBER 2016.

3

Acronyms and Abbreviations

CUEC	Complementary User Entity Controls
DLA	Defense Logistics Agency
iRAPT	Invoice, Receipt, Acceptance, and Property Transfer
NAVFAC SW	Naval Facilities Engineering Command Southwest
NIST	National Institute of Standards and Technology
SSC Pacific	Space and Naval Warfare Systems Center Pacific
SWRMC	Southwest Regional Maintenance Center Pacific Fleet

Whistleblower Protection
U.S. Department of Defense

The Whistleblower Protection Enhancement Act of 2012 requires the Inspector General to designate a Whistleblower Protection Ombudsman to educate agency employees about prohibitions on retaliation, and rights and remedies against retaliation for protected disclosures. The designated ombudsman is the DoD Hotline Director. For more information on your rights and remedies against retaliation, visit www.dodig.mil/programs/whistleblower.

For more information about DoD IG reports or activities, please contact us:

Congressional Liaison
congressional@dodig.mil; 703.604.8324

Media Contact
public.affairs@dodig.mil; 703.604.8324

For Report Notifications
http://www.dodig.mil/pubs/email_update.cfm

Twitter
twitter.com/DoD_IG

DoD Hotline
dodig.mil/hotline


INSPECTOR GENERAL
INTEGRITY
EFFICIENCY
DEPARTMENT OF DEFENSE

DEPARTMENT OF DEFENSE | INSPECTOR GENERAL

4800 Mark Center Drive
Alexandria, VA 22350-1500
www.dodig.mil
Defense Hotline 1.800.424.9098