ITS# E-01159

Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by Battelle *Since 1965*

Cause Analysis Report for Payment to a Fraudulent Subcontractor

PNNL Cause Analysis Level 2

April 2017

KH Pryor (Lead)
SJ Anderson
DP Mendoza

U.S. DEPARTMENT OF ENERGY

Prepared for the U.S. Department of Energy
under Contract DE-AC05-76RL01830

Executive Summary

The Manager of Financial Operations, Iris Anderson, chartered a team to conduct a Level 2 root cause analysis to understand the cause(s) for the issue of an invoice payment to a fraudulent entity posing as a PNNL subcontractor. This issue was determined to be of MEDIUM significance. In November 2016, a fraudulent entity requested an Authorized Clearing House (ACH) banking change while posing as an employee of Fowler General Construction, Inc. (Fowler). This request was completed and returned to the Accounts Payable (AP) group, was processed in accordance with the Vendor Management Process Desk Guide and the new (and fraudulent) banking information was updated in the Vendor Master File in the Purchase and Expense System (PES). Following payment of an invoice in December, 2016, the fraudulent entity withdrew the funds and closed the bank account. In January 2017, Fowler noticed that they had not received payment on their invoice, contacted PNNL, and it was subsequently discovered that payment had incorrectly been made to the bank account of the fraudulent entity.

Problem Statement: An invoice payment was believed to have been made to the bank account of a PNNL subcontractor on December 16, 2016; on January 12, 2017, it was subsequently discovered that the payment had incorrectly been made to a bank account of a fraudulent entity posing as a legitimate subcontractor that was set up in the PNNL Vendor Master File.

Results

The cause analysis yielded a direct cause and one root cause.

Direct Cause: The AP Vendor Coordinator verified the information on the ACH request that was specifically required by the Vendor Management Process Desk Guide against the information in the Vendor Master File; the AP Vendor Coordinator unknowingly changed the bank account to the one that belonged to the fraudulent entity and the invoice was paid by ACH into that bank account.

The AP Vendor Coordinator validated the information on the ACH request form that was required by the Vendor Management Process Desk Guide, which consisted of checking the name of the company, the address of the company and the Taxpayer identification (ID) number [or social security number (SSN)] against the data in the Vendor Master File. This information matched that found in the vendor's record. According to the Vendor Management Process Desk Guide, when the vendor name, address and Taxpayer ID/SSN match what is currently in the Vendor Master File, the change in banking information is then entered into the Vendor Master File. Changes in Points of Contact (POCs) (or their contact information) are not required to be verified by phone or email with the listed POC. The email address is not required to be verified against existing email addresses in the Vendor Master File.

Root Cause: BSD Management had a primary focus on controls over internal fraud risks in response to DOE's annual risk statements in the Accounts Payable area (which did not specifically address external fraud risks), and based on the majority of previous experience involving internal fraud. Consequently, the controls for the identification, detection and response to evolving fraudulent activities by external criminal entities in the Vendor Management Process were less than adequate.

OMB Circular A-123 is incorporated by reference in PNNL's prime contract under the CRD for DOE O 413.1B which defines management's responsibility for enterprise risk management and internal control (including fraud; both internal and external). These requirements are broad in nature and do not specifically address fraudulent activities by external sources. Annually, DOE provides risk statements for each financial process area with the expectation that management perform a risk assessment, taking both the DOE risks statements and any additional PNNL-generated risk statements into account to reasonably assure that risk for each financial area is identified and controls are in place to mitigate the identified risks to the extent management deems appropriate. DOE provided risk statements in the Accounts Payable process area (CR2301 and CR2309) that cover improper, invalid or untimely updates to the Vendor Master File and improper, invalid or untimely payments. The mitigating controls identified for these risk statements (C399, C428 and C435) focused on untimely payments, tracking of improper payments and segregation of duties, and not on invalid payments (e.g., payments to fraudulent subcontractors).

PNNL focused efforts related to fraud identification and prevention on internal sources, such as segregation of duties, unethical behavior by employees, and kickbacks to employees from subcontractors and vendors. There is no program or organization that is responsible for periodically monitoring external information sources (e.g., FBI website, IRS website, National Contract Management Association website, Association of Certified Fraud Examiners website) for the existence of potential threats or scams currently being perpetrated by external entities. These potential threats and scams are increasing in frequency and becoming more sophisticated. BSD relies on individual staff members to identify and respond to potential fraudulent activity by external sources; however, this is not a written expectation.

There are no upper-level policies or procedures that clearly cover the identification, detection and response to potential fraud from external sources in relation to the Vendor Management Process. Acquisitions Guide (AG)-01, *PNNL Procurement Policy Manual*, states that Battelle will be "sensitive to indications of unlawful behavior or personal and/or organizational conflicts of interest by offerors, subcontractors and Battelle personnel." AG-37, *Invoice Reviews*, describes the process used by AP and Contracts to review and approve invoices; it does not include reviews of changes in banking information or vendor POCs. The Vendor Management Process Desk Guide used by the AP Vendor Coordinator did not include sufficient controls on the ACH banking changes to detect a fraudulent request. The Vendor Management Desk Guide describes how to make the change in the PES, but there is no caution to verify the legitimacy of the request.

Contents

1.0 Background

1.1 Vendor Management/Payment Process

The PeopleSoft Purchase and Expense System (PES) uses a common database consisting of the Vendor Maintenance, Purchase Requisitions (PR), Purchase Orders (PO), Receiving, and Accounts Payable (AP) modules. Purchase Orders are prepared by a Contracts Specialist, services are rendered by the vendor, and the vendor submits an invoice which is reviewed and approved for payment through the PES.

Invoice processing is described in Acquisition Guidelines (AG) 37, *Invoice Review*. This AG describes the requirements and responsibilities for all participants involved in the invoice review process. Invoices are reviewed to prevent any payments that are not authorized, allocable, allowable and reasonable based on the contract. When an invoice is received, an AP Administrator verifies the invoice against the information provided on the PO, checks for duplicates, and verifies labor rates, indirect rates and travel expenses against the terms of the contract. The AP Administrator is responsible for entering the invoice and supporting information into the PES to route for review and approval by the Contracts Assistant, the Technical Oversight Representative (TOR), and the Contracts Specialist. Upon confirmation of invoice approval, AP releases the voucher for payment of the approved amount according to the net terms of the contract.

PNNL currently has over a thousand subcontractors actively performing work. Payments for services rendered are set up via three mechanisms: wire transfers, paper checks, or Authorized Clearing House (ACH) payments.

Wire transfer is a method of electronic funds transfer from one person or entity to another. Wire transfers are the electronic payment method used to primarily make payments to foreign vendors. The following controls are in place around wire transfers:

- The AP Manager reviews and approves each wire transfer.
- Treasury dispatches actual payments to the bank (to provide separation of duties).
- The banking information on the invoice is compared to the banking information selected in the PES (banking information is provided on ~95% of invoices paid via wire).
- Wire transfers go through strict Office of Foreign Assets Control (OFAC) review and compliance.

The paper check is a form of payment that draws money directly from a checking account. The "payer" -- the writer of the check -- writes the name of the "payee" on the "pay to the order of" line and signs the check on the signature line (electronically-generated signature). The following controls are in place around the paper check process:

- The PES sequentially numbers the checks on the check run and the number of checks are manually counted and compared to the expected number of checks to run. Checks are run

by one staff member and the review/count is performed by a second person.

- The check stock is secured in a locked cabinet and the ability to print checks is limited to specifically designated printers (the printer drawer requires a key and the printer requires special software).
- Positive pay service (an automated fraud detection tool offered and used by the bank) are implemented for the bank to honor the check.
- Checks are monitored by AP staff while the checks process through the check sealer.

ACH payment is an electronic network for financial transactions in the United States. ACH processes large volumes of credit and debit transactions in batches, and is the electronic payment method used for domestic payments. The following controls are in place for ACH payments:

- The AP Manager reviews and approves ACH payments, while the Treasury Department dispatches actual payments to the bank (to provide separation of duties).
- The banking information on the invoice is compared to the banking information selected in the system (banking information is provided on ~40% of invoices paid via ACH).
- The ACH pre-notification process ("$0 ping") is used to make sure that the account/routing information is valid prior to the first payment. The bank is only required to verify the authenticity of the account, and does not verify the name on the account. Management was operating under the incorrect assumption that this control was providing name validation.
- Automated ACH payment notification is sent via email by the PES to the vendor upon payment. This notification includes payment date, amount, and the last 4 digits of the account to which the payment was remitted.

There are two Vendor Coordinator positions within BSD: the Contracts Vendor Coordinator and the AP Vendor Coordinator. The Contracts Vendor Coordinator reports to the Operations and Analytics Manager in the Contracts organization. The AP Vendor Coordinator reports to the AP Manager in the Payroll and Payables/Financial Operations organization. The Contracts Vendor Coordinator sets up new vendors in PES; the AP Vendor Coordinator primarily makes changes to vendor information in PES in response to changes that occur during processing of invoices. The duties of the two positions overlap; both have the same Role-Based Access Controls (RBAC) in PES. Currently, the AP Vendor Coordinator is performing the duties of both Vendor Coordinator roles due to staff turnover and delays in hiring a new Contracts Vendor Coordinator.

The Vendor Management Process Desk Guide provides written guidelines for the creation, maintenance and control of the Vendor Master File within the PES. This desk guide is used by both the Contracts Vendor Coordinator and the AP Vendor Coordinator; this role is controlled through the Application Role Access Request and is granted by the AP Manager. The desk guide states that the AP Manager is responsible for the oversight of the Vendor Management Process.

The desk guide also cautions:

> *Keeping the data within the Vendor Master File clean is important for the Purchase to Pay process to be successful. An inaccurate, unclear, or disorganized master vendor file can spell disaster. A poorly maintained master vendor file can lead to duplicate or erroneous payments, missed discounts, uncashed checks, unapplied credits, tax reporting errors, and fraud.*

The AP Vendor Coordinator is responsible for the input of any changes to ACH payment information in the PES system when they are requested by a vendor. The vendor notifies the AP Office using the email box AP.Invoices@pnnl.gov that a change to the ACH information is needed, and either the AP Vendor Coordinator or AP Administrator sends a blank ACH form to the vendor to populate with the correct business information and the requested banking change(s). The vendor returns the completed ACH form to the AP Office using the email box AP.Invoices@pnnl.gov and the AP Vendor Coordinator verifies that the vendor name, address and taxpayer identification number (or Social Security Number) are correct. Once this information is verified, the AP Vendor Coordinator enters the new ACH information from the form into the Vendor Master File. The previous information is not deleted from the vendor's record in the Vendor Master File; the new information is added to the existing record (including updates to the point of contact (POC) and email address for the Vendor).

1.2 ACH Change Request from Fowler General Construction, Inc.

Fowler General Construction, Inc. (Fowler) has been a subcontractor at PNNL since 2007, and has worked on numerous construction projects on the PNNL campus. An ACH was set up with Fowler when they initially began working for PNNL as a subcontractor. Over the past ten years, there have been a total of three bank account changes for Fowler: one that was initiated by a bank notification to update the routing number; one that was initiated by Fowler to change bank accounts; and the most recent one that was initiated by the fraudulent entity to change bank accounts (the subject of this cause analysis).

In May 2016, a contract was awarded to Fowler for the construction of the PNNL Collaboration Center. The first invoice from Fowler for the Collaboration Center work was received on June 21, 2016, with payment occurring on July 20, 2016 via ACH to their designated bank account.

On November 9, 2016, a request was made via email to the Procurement Director to change the bank account for Fowler's ACH payments. The email included the company logo and an email address of accounts@fowlergcgroup.com. The Procurement Director recognized the Fowler logo on the email and forwarded the email to the AP Manager for action. The Procurement Director typically received emails from vendors and would forward AP-related requests to the AP Manager; however, this was the first email received by the Procurement Director requesting an ACH form.

The AP Manager received the forwarded email request but did not immediately recognize the name of the subcontractor. The AP Manager verified that Fowler was listed as a vendor in the

Vendor Master File and then sent a blank ACH form to the requestor by email. The requestor completed the ACH form and returned it by email directly to the AP Manager with a request to be notified when the information was updated and the next payment was due. The AP Manager forwarded the email with the completed form to the ^AP Vendors (email) mailbox to be updated in the Vendor Master File.

The AP Vendor Coordinator was the only individual at the time that had the ability to make ACH changes in the Vendor Master File (the same individual was performing the duties of both the Contracts and AP Vendor Coordinator roles due to staff turnover and delay in hiring a new Contracts Vendor Coordinator). The AP Vendor Coordinator verified the name and address of the subcontractor and the tax ID number as required by the Vendor Management Process Desk Guide. The AP Vendor Coordinator then updated the Vendor Master File with the new ACH information, and added the requestor's name and email as another POC for Fowler.

After the vendor record was updated with the ACH change, the pre-notification process was initiated by the Vendor Coordinator. This consisted of sending a "$0 ping" to the bank to verify that the account was valid. The bank is only required to verify the authenticity of the account; the name on the account is not checked or verified. On November 17, 2016, the pre-notification ("$0 ping") was sent to the new bank with the regularly scheduled ACH file; after 10 days, with no notification of change from the bank, the PES system set the ACH pre-notification to "confirmed" and the new banking information could be used.

On December 16, 2016, a Fowler invoice was paid by ACH to the new bank account. Both POCs listed in Fowler's vendor record (the legitimate POC and the new fraudulent entity) were sent an automatic notification of the payment. The fraudulent requestor withdrew the funds from the new bank account within a few days and closed the account.

Fowler normally verifies that payment is received within a few days of notification. However, in December 2016, they did not follow their normal process due to the holidays. During their bank reconciliation in January 2017, Fowler noticed that the email notification of payment for the invoice had the wrong bank number. On January 12, 2017, Fowler's Controller contacted PNNL AP by phone to inform AP that they had not received their invoiced payments. The AP Administrator reviewed the vendor record in PES and informed Fowler that the payment had been submitted to the new bank account. Fowler responded that the requestor on the ACH form was not an employee of Fowler and the bank change was not valid.

The AP Administrator informed Fowler they would investigate the situation and immediately notified the AP Manager. The AP Manager assessed the situation, reviewed the vendor history, and examined pertinent emails, then met with Finance and Contracts management to discuss immediate actions to be taken. Treasury also immediately notified the bank of the fraudulent transactions. Appropriate notifications were made to senior management, Office of Audit Services, and the Office of General Counsel, and a number of compensatory actions were promptly initiated.

1.3 Requirements and Audits/Issues Related to Fraud Prevention/Detection

Compliance with the Contract Requirements Document (CRD) of DOE Order 413.1B is required by PNNL's operating contract with DOE. This CRD incorporates the Office of Management and Budget (OMB) Circular A-123 by reference. OMB Circular A-123 provides guidance on improving the accountability and effectiveness of programs and operations by establishing, assessing, correcting, and reporting on internal control (including fraud, both internal and external). A-123 establishes an assessment process based on the Government Accountability Office's (GAO) Standards for Internal Control in the Federal Government (the "Green Book"), and defines management's responsibilities related to internal control and the process for assessing internal control effectiveness. The A-123 program stipulates the assessment process and the methodology management uses to support its assertion as to the effectiveness of the internal controls over financial reporting. The Green Book outlines the principles of internal control based on the integrated framework developed by the Committee of Sponsoring Organizations of the Treadway Commission (COSO). Principle 8 covers assessing fraud risk, and states that "Management should consider the potential for fraud when identifying, analyzing and responding to risks." The attributes that contribute to the design, implementation and operating effectiveness of this principle are: (1) types of fraud, (2) fraud risk factors and (3) response to fraud risks.

These requirements are broad in nature addressing fraud as a whole, not specifically addressing fraudulent activities by external sources. PNNL has focused their efforts on the identification, detection and prevention of internal fraud.

PNNL has developed the A-123 program in order to meet three primary objectives, as described in the PNNL Finance Manual: (1) improve the effectiveness and efficiency of financial, accounting, and other operations which materially impact the PNNL financial statements; (2) ensure compliance with OMB A-123 Appendix A requirements; and (3) integrate OMB A-123 Appendix A requirements with current self-assessment, assurance and governance processes. Annually, DOE flows down a set of risks to contractors that must be identified and mitigated via internal controls. PNNL is also expected to identify any additional risks and develop mitigating internal controls that may be unique to PNNL.

An Internal Audit was conducted in June 2014 which assessed PNNL's overall risk and control procedures for fraud prevention and detection. The scope included an assessment of the design and operation of PNNL financial, human resources and legal controls to prevent and detect fraudulent activities over the period from October 2012 through January 2014. This represented the first internal audit to conduct a penetration assessment of PNNL's internal fraud risk and controls. The assessment concluded that appropriate policies, procedures, and controls to prevent and detect fraud were in place, but also recommended that PNNL develop an integrated ethics and compliance, or anti-fraud plan to address all aspects of fraud risk management to further strengthen existing controls. PNNL's fraud detection and prevention measures have primarily

focused on internally-generated fraudulent activities (i.e., by employees or insiders); this is consistent with the types of fraudulent activities that have been detected to date.

In December 2015, external fraudulent entities solicited quotations for "consumer electronics" using the PNNL Procurement Director's name, as well as other Contracts Specialists names. This solicitation was sent out by fax transmittals to thousands of vendors. A number of vendors responded to the fraudulent entities, who then submitted purchase orders for electronics using the Contract Manager's name. The vendors requested pre-payment from the fraudulent entity, but the entity would respond that pre-payment was not allowed under Federal government policy, and that payment would be made at the time of receipt and acceptance of the goods. Approximately ten vendors shipped consumer electronic goods to the fraudulent entity. The solicitations have continued on a monthly basis since December 2015, primarily using the PNNL Procurement Director's name. The DOE Office of the Inspector General and the Federal Bureau of Investigation (FBI) were notified and investigation of this external fraudulent activity is on-going. This issue also served to increase awareness on the part of Contracts and AP management and staff of fraudulent activities that could be perpetrated by external criminal entities.

2.0 Scope and Approach

2.1 Scope

The cause analysis team was requested to determine the causes for the event that led to improper payment to a fraudulent entity that was posing as a subcontractor to PNNL. This issue was determined to be MEDIUM significance, requiring a Level 2 root cause analysis. The scope of this cause analysis was limited to PNNL's response to the ACH change request by the fraudulent entity. A separate investigation is being conducted by the Office of the Inspector General and the Department of Justice to determine how the fraudulent entity obtained the relevant information to make the ACH change request in the first place.

2.2 Approach

The cause analysis team charter authorized Kathy Pryor to be the team lead, supported by Stephanie Anderson and Donald Mendoza. During the course of the investigation, the team reviewed available documents (Appendix A) and interviewed 16 PNNL staff members and one subcontractor (Appendix B).

3.0 Methodology

The team developed a problem statement from the Charter, as shown below. They then reviewed relevant documents, conducted interviews, and used the analysis techniques listed below to identify the causal factors associated with the payment to the fraudulent entity.

To provide a comprehensive analysis, the following tools were used in combination to derive the causes:

- MORT analysis (Appendix D)
- Hazard-Barrier-Target analysis (Appendix E)
- Why Analysis (Appendix F)

Problem Statement: An invoice payment was believed to have been made to the bank account of a PNNL subcontractor on December 16, 2016; on January 12, 2017, it was subsequently discovered that the payment had incorrectly been made to a bank account of a fraudulent entity posing as a legitimate subcontractor that was set up in the PNNL Vendor Master File.

4.0 Results

The cause analysis yielded a direct cause and one root cause, as described below.

4.1 Direct Cause

Direct Cause: The AP Vendor Coordinator verified the information on the ACH request that was specifically required by the Vendor Management Process Desk Guide against the information in the Vendor Master File; the AP Vendor Coordinator unknowingly changed the bank account to the one that belonged to the fraudulent entity and the invoice was paid by ACH into that bank account.

DOE cause codes:

- **A5B2C08 –** Communications LTA | Written communication content LTA | Incomplete/situation not covered.
- **A3B2C04 –** Human performance LTA | Rule Based Error | Previous success in use of rule reinforced continued use of rule.

Relevant Facts:

- The AP Vendor Coordinator validated the information on the ACH request form that was required by the Vendor Management Process Desk Guide. The AP Vendor Coordinator checked the name of the company, the address of the company and the Taxpayer identification number against the data in the Vendor Master File. This information matched that found in the vendor's record.
- The AP Vendor Coordinator received on-the-job training from the previous Contracts Vendor Coordinator. The previous Contracts Vendor Coordinator had executed a number of ACH

banking change requests in the past and validated the same information that was specified in the Vendor Management Process Desk Guide.

- Both the AP Desk Guide and Vendor Management Process Desk Guide are "how to" documents written with step by step instructions (including screenshots) describing how to execute various AP and Vendor Coordinator tasks.
- The section of the Vendor Management Process Desk Guide that covers ACH change requests does not require verification of the request by email or phone call with the listed vendor POC. When the vendor name, address and Taxpayer ID/SSN match what is currently in the Vendor Master File, the change in banking information is entered into the Vendor Master File.
- The Fowler request was made by a new (and fraudulent) POC with a different email address (and a different domain name) than the one used by the listed Fowler POC. The listed Fowler POC's email address used the domain name @fowlergc.com, while the fraudulent entity used an email address with the domain name @fowlergcgroup.com. Changes in POCs (or their contact information) are not required to be verified by phone or email with the listed POC. The email address is not required to be verified against existing email addresses in the Vendor Master File.
- The ACH pre-notification process ("$0 ping") that was used to make sure that the account/routing information was only verified the authenticity of the account, and did not verify the name on the account. Management was operating under the incorrect assumption that this control was providing name validation.

4.2 Root Cause

Root Cause: BSD Management had a primary focus on controls over internal fraud risks in response to DOE's annual risk statements in the Accounts Payable area (which did not specifically address external fraud risks), and based on the majority of previous experience involving internal fraud. Consequently, the controls for the identification, detection and response to evolving fraudulent activities by external criminal entities in the Vendor Management Process were less than adequate.

DOE cause codes:

- **A4B1C01 –** management problem |management methods LTA |management policy guidance/expectations not well-defined, understood or enforced.

Relevant Facts:

- OMB Circular A-123 is incorporated by reference in PNNL's prime contract under the CRD for DOE O 413.1B which defines management's responsibility for enterprise risk management and internal control (including fraud; both internal and external). These requirements are broad in nature and do not specifically address fraudulent activities by

external sources. PNNL focused their efforts on the identification, detection and prevention of internal fraud.

- The OMB Circular A-123 controls for the Vendor Management Process focus on the Vendor Master File, and the only control listed relies on segregation of duties through the RBAC roles for the Vendor Coordinator and Wire Banking Maintenance (i.e., Treasury). There is no control listed for ACH disbursements.
- The Acquisitions M&OP owns the requirements for the Vendor Management Process, including requirements for AP to make timely and accurate interim and final payments to vendors in accordance with subcontract terms. The Acquisitions M&OP lists the PNNL procurement policies, AGs and the AP Desk Guide as key implementations. There are no upper-level policies or procedures that clearly cover the identification, detection and response to potential fraud from external sources in relation to the Vendor Management Process. The Vendor Management Process Desk Guide is not listed as an implementation method.
- AG-01, *PNNL Procurement Policy Manual*, states that Battelle will be "sensitive to indications of unlawful behavior or personal and/or organizational conflicts of interest by offerors, subcontractors and Battelle personnel." There is no specific discussion of the potential for various mechanisms of fraudulent activity by external entities or elaboration regarding "indications of unlawful behavior."
- AG-37, *Invoice Review*, "delineates the requirements and responsibilities for all participants involved in the invoice review process. ...invoices are reviewed to prevent paying anything other than authorized, allowable and reasonable amounts based on the contract." This AG states that AP reviews invoices for vendor names, tax documentation, contract price, period of performance, labor rates, etc. This AG does not describe any AP review of the banking information or the POC for the vendor.
- The PNNL Finance Manual, Section 11.8, states the requirements for review of domestic invoices by AP and Contracts. The responsibilities listed for AP in the invoice review process do not include a review of the banking information.
- There is no AG that covers the process for responding to vendor requests for changes in banking information, regardless of the method used to pay invoices.
- The Vendor Management Process Desk Guide used by the AP and Contract Vendor Coordinators did not include sufficient controls on the ACH banking changes to detect a fraudulent request. The Vendor Management Desk Guide describes how to make the change in the PES. The company name, address, Social Security Number or Taxpayer ID number must match what is on file in PES. There is no caution to verify the legitimacy of the request.
- The Vendor Management Process Desk Guide was written and maintained by both the Contracts and AP Vendor Coordinators; it is housed on a SharePoint site and not formally controlled or approved by management. The Vendor Management Process Desk Guide

states that "the Accounts Payable manager is responsible for the oversight of the vendor process, which includes any changes to policy."

- Because ACH changes are numerous and routine, there is a certain risk tolerance in executing these changes. There are approximately 50 ACH banking changes made to existing vendor records on a monthly basis. Resources that would be needed to verify all banking changes would be substantial.
- The AP Administrator uses a "Paperless Checklist" for vouchering and an "AP Releases Checklist" for final AP approval prior to releasing a payment to a vendor. Both of these checklists include a step to verify that the banking information selected on the voucher matches that on the invoice (if provided). If PNNL has not paid the vendor in over one year, AP contacts the vendor to make sure that the ACH banking information in the Vendor Master File is still valid.
- Transition of key staff out of both the AP and Contracts organizations resulted in the AP Vendor Coordinator assuming additional responsibilities while maintaining the normal work load.
- A replacement Contracts Vendor Coordinator was hired and was trained by the AP Vendor Coordinator. This replacement Contracts Vendor Coordinator only stayed in this position for a few months before leaving PNNL; the AP Vendor Coordinator is currently filling both Vendor Coordinator roles on an interim basis.
- The previous AP Manager had 9 years of experience in this position and was familiar with the ACH and bank change processes; this manager performed as a back up to the AP Vendor Coordinator and had made several banking account changes in the PES. The current AP Manager has been in the role for approximately 1.5 years and has since stopped the practice of backing up the AP Vendor Coordinator in order to provide better segregation of duties.
- The Management & Operating Subcontract Reporting Capability (MOSRC) is an initiative that provides the ability to accurately report the UNCLASSIFIED 1st-tier subcontracting activity of the Department of Energy (DOE)'s M&O contractors to the Small Business Administration (SBA) and the general public. This new reporting requirement has prompted significant clean-up efforts in the Vendor Master File by Contracts and AP. Due to this effort, the Vendor Management Process is being streamlined, and PNNL will be linked to the System for Award Management (SAM), which will minimize the amount of manual input into the Vendor Master File.
- PNNL focuses efforts related to fraud identification and prevention on internal sources, such as segregation of duties, unethical behavior by employees, and kickbacks by subcontractors and vendors to employees. The HDI Work Control - *Basic Staff Practices* includes a section on Business Ethics and Staff Conduct; it is focused on the expectations for PNNL staff. Staff members also are required to complete Course 1962, PNNL Ethics and Conduct Training.

- There is no program or organization that is responsible for monitoring external information sources (e.g., FBI website, IRS website, National Contract Management Association website, Association of Certified Fraud Examiners website) for the existence of potential threats or scams currently being perpetrated by external entities. There is no routine monitoring of emerging scams or threats from external sources. BSD relies on individual staff members to identify and respond to potential fraudulent activity by external sources.
- The Acquisitions M&OP extent of deployment assessment focuses on AP invoice reviews as described in AG 37; AP reviews contracts and invoices to make sure the amounts match prior to payment; RBAC roles are delegated so that appropriate accesses are given and to maintain segregation of duties. The extent of deployment does not expand the invoice reviews to include a review of the changes in banking information to be used.
- OMB Circular A-123 states that management is responsible for implementing management practices that identify, assess, respond, and report on risks. Annually, DOE provides risk statements for each financial process area with the expectation that management perform a risk assessment taking both the DOE risks statements and PNNL generated risk statements that are not captured into account to reasonably assure that risk for each financial area is identified and controls are in place to mitigate the identified risks to the extend management deems appropriate. DOE provided risk statements in the Accounts Payable process area (CR2301 and CR2309) that cover improper, invalid or untimely updates to the Vendor Master File and improper, invalid or untimely payments. The mitigating controls identified for those risk statements (C399, C428 and C435) focused on untimely payments, tracking of improper payments and segregation of duties, and not on invalid payments (e.g., payments to fraudulent subcontractors).
- Contract Clause I-9, FAR 52.203-13, Contractor Code of Business Ethics and Conduct was added to PNNL's operating contract in October 2016, and was assigned to the Office of General Council (OGC). This clause requires that the "Contractor must exercise due diligence to prevent and detect criminal conduct." This clause, and the implementations listed in ROD 1136, focus primarily on fraud and unethical behavior by internal sources (employees).
- An Internal Audit on fraud risk assessment, conducted in 2014, identified a group of mechanisms and documents that, when taken collectively, provided reasonable protection from fraud from internal sources. This report recommended that management develop an integrated ethics and compliance/anti-fraud plan. The action was closed in January 2016 by stating that management had explored the options, and the development of such a plan was assigned to the OGC and Internal Audit. Development of this plan is currently in progress; the focus of this plan is on unethical behavior or fraudulent activity by internal sources.
- Most experience with previous fraudulent activity at PNNL has involved activities perpetrated by internal sources. However, recent fraudulent activity (discovered in December 2015) has involved an external entity posing as the PNNL Procurement Director and sending out fraudulent solicitations for quotes on consumer electronics. When vendors

responded to these fraudulent solicitations, the external entity would negotiate a purchase order with no pre-payment option and the vendors would ship the goods to the fraudulent entity. PNNL's response focused on informing Federal and law enforcement authorities, and the possibility of payment of false invoices to the fraudulent entity; Contracts and AP management concluded that a false invoice would be detected by existing controls and would not be paid.

Appendix A – List of Documents Reviewed

1. ACH Vendor/Miscellaneous Payment Enrollment Form
2. Vendor Management Process Desk Guide
3. Accounts Payable Manual (AP Administrator Desk Guide)
4. AP Paperless Checklist and AP Releases Checklist
5. E-mail Correspondence relating to ACH change request
6. AP Department Self Assessments
7. Office of Audit Services Fraud Risk Assessment Audit IA2014-16., 3.C.1.B Vendor Management-Audit Title: Fraud Risk Assessment
8. DOE Accounting Manual, Ch. 6
9. PNNL Finance Manual, Section 6.8.1 - Special Bank Account Agreement, Section 11 - Acquisitions
10. AG-37, PNNL Invoice Review
11. AG-01, PNNL Procurement Policies Manual
12. FAR 52.203-13, Contractor Code of Business Ethics and Conduct (Contract Clause I-9)
13. ROD 1136, Rev. 1, Clause I-9 FAR 52.203-13 Contractor Code of Business Ethics and Conduct (Oct 2015)
14. ROD 454, Rev. 6, 1830 Contract? Appendix B Special Financial Institution Account(s) Agreement
15. Payables Management Narrative, PNNL A-123
16. Committee of Sponsoring Organizations (COSO)
17. OMB, Circular A-123, July 15, 2016
18. GAO-14-704G, Standards for Internal Control in the Federal Government (Green Book), Government Accountability Office, September 2014
19. DOE CRD O 413.1B - OMB Circular A-123
20. Acquisitions Management & Operations Program Description
21. OGC Management & Operations Program Description
22. Acquisitions M&OP Extent of Deployment Report, 3rd Trimester for FY16
23. Acquisitions M&OP Extent of Deployment Report, 1st Trimester for FY17
24. HDI Roles, Responsibilities, Accountabilities, and Authorities (R2A2s) for SMEs, Expert Delivery for M&O programs, Acquisitions, OGC
25. Cause Analysis Report for Weakness in Cash Disbursements and Reconciliation

Appendix B – List of Interviews Conducted

Staff Member	Title
Iris Anderson	Manager, Financial Operations
Chris Armstrong	Manager, Payroll and Payables
Kerry Bass	Finance and Accounting Professional (Financial Assurance and Risk Assessment)
Aimee Bergeson	Fowler General Construction, Inc.
Vincent Branton	General Counsel
Lindsie Canales	Manager, Accounts Payable
Cindy Carpenter	AP Administrator
Kevin Ensign	Director, Office of Audit Services
Garrett Hyatt	Contracts Specialist
Jeff Leaumont	Manager, Contracts (Procurement Director)
Grace Lester	Contracts Vendor Coordinator (retired)
Erlan Leitz	Manager, Financial Assurance and Risk Assessment
Naomi Love	AP Vendor Coordinator
Carol MacInnis	Acquisitions M&O Program Manager
Loren Peterson	Manager, Accounting and Receivables (previous Manager, Payroll and Payables)
Mike Schlender	Deputy Director for Operations/Chief Operating Officer
Jackie Steele	Finance and Accounting Professional (EBSD/PCSD Business Office)(previous Manager, Accounts Payable)
Susan Turner	Manager, Operations and Analytics (Contracts)
Suzanne Williams	Finance and Accounting Professional (Treasury Services)

Appendix C – Cause Analysis Charter

PNNL Cause Analysis Charter
Fraudulent Payment to Posed subcontractor

Iris Anderson, Financial Operations Manager has requested assistance in conducting a Level 2 root cause analysis to better understand the issues associated surrounding the fraudulent payment for a subcontractor event. This charter defines the scope of the cause analysis effort and the conditions necessary for its completion by the analysis team. This issue was deemed to be of MEDIUM significance.

Background
In January of 2016, a request for proposal (RFP) was submitted by PNNL contracts requesting bids for a design/build project for a collaboration center. The contract was awarded to Fowler General Construction Inc., in May of 2016. Fowler has been a subcontractor for PNNL since 2007 and 58 purchase orders have been dispatched to them with payments of approximately $20 million made to them. Fowler had the vendor payment infrastructure already in place at PNNL through an Automated Clearing House (ACH) mechanism for payments to be made to a designated bank account. Design activities commenced with an architect firm, TVA Architects, out of Portland, Oregon, a subcontractor to Fowler on this contract, immediately after notice to proceed was given. The first invoice was received on 6/21/16 with payment occurring on 7/20/16. Four additional payments were made to Fowler under this award prior to the fraudulent bank account that was set up in mid-November.

Issue Description
On January 12th, 2017, accounts payable (AP) received a call from a subcontractor (Fowler General Construction Inc.) requesting payment for services rendered. The AP administrator pulled up the vendor account showing that the payment was deposited on 12/16/16, but noted that the banking account had changed in mid-November and the deposit was made to this new account. The AP administrator conveyed this information to the subcontractor along with the contact name that initiated the bank account change. The subcontractor indicated the contact was not an employee of Fowler General Construction Inc. and the bank change was not valid.

Cause Analysis Team
The cause analysis will be performed by the Lead Cause Analyst, Kathy Pryor and supported by Donny Mendoza (Lead Cause Analyst-in training), and Stephanie Anderson (Finance Assurance and Risk Assessment). The Team is chartered to perform a Level 2 root cause analysis using appropriate analytical techniques.

Authorized Scope and Timing of the Analysis
The Team is authorized to investigate the issues through document reviews, field observations, and interviews, as necessary to identify and report the cause(s) of the issues. This effort will begin 1/30/17 and will conclude with a final approved report on or before 2/25/17.

The Lead Cause Analyst may request additional specific subject matter expertise and consultation to support the analysis, as needed. The Lead Cause Analyst will immediately communicate to the Issue Owner any potential scope changes, including the need for:

- Increasing/decreasing the boundaries of the analysis
- Additional team members
- Additional time to conduct a thorough and defensible analysis

Expected Products and Activities

To successfully conclude this cause analysis, the Lead Cause Analyst shall:

- Identify the causes (direct, root, and any contributing) associated with the issues using accepted analytical techniques;
- Provide verbal progress updates at least weekly (or as requested) to the Issue Owner or delegate;
- Provide draft results in a briefing to the Issue Owner on or before (2/10/17);
- Submit a report for approval to the Issue Owner on or before (2/22/17).

If the Team discovers conditions requiring immediate compensatory measures, regardless of their relationship to the analysis (such as for the protection of staff or the public) the Lead Cause Analyst will communicate these to the Issue Owner immediately upon their discovery.

Approval History for: Fraudulent Payment to Posed Subcontractor CA Charter

Final Process State: APPROVED

Name		Activity Name	Date
☒ ACCEPTED	Pryor, Kathryn H	Approval	1/25/2017 5:54:52 AM
☒ ACCEPTED	Andersen, Iris E	Approval	1/26/2017 9:04:52 AM

* All actions are stored digitally and viewable at https://approvals.pnl.gov/ProcessView.aspx?pid=2602106

Appendix D. MORT Analysis

Key:	
Green	= No weaknesses identified
Red	= Weaknesses identified
Grey	= Does not apply
Blue	= Insufficient information available

A – Management System Factors		
MA1	Policy LTA	Is there a written up-to-date policy or policies with a broad enough scope to address the problems likely to be encountered during the conduct of work in the facility? Does the policy cover such major items as personnel, cost, quality, efficiency, and legal compliance? Can the policy be implemented without conflicting with other policies?
Conclusion: BSD Management did not clearly define adequate controls regarding the identification, detection and response to potential fraudulent activities by external entities in the Vendor Management Process. There are no upper-level policies that address expectations for fraudulent activities by external entities with respect to the Vendor Management Process. Previous issues surrounding fraudulent activities stemmed from internal problems, focusing EOD and self-assessments on measures to keep internal fraudulent activities from occurring. Policies and requirements that were followed focused on internal threats.		

Section #	Title	Causal Factors/Observations	Cause Reference
A1	Are policies up-to-date?	PNNL focuses efforts related to fraud identification and prevention on internal sources, such as segregation of duties, unethical behavior by employees, kickbacks by subcontractors and vendors to employees.	
A2	Are policies written?	PNNL focuses efforts related to fraud identification and prevention on internal sources, such as segregation of duties, unethical behavior by employees, kickbacks to employees by subcontractors and vendors.	

A3	Are policies based on adequate risk assessment?	EOD and self-assessments did not focus on external criminal fraudulent activity. The Acquisitions M&OP extent of deployment assessment focuses on AP invoice review process as described in AG 37. The risk has been focused on internal fraudulent activities. PNNL's A-123 risk assessment and mitigating controls for AP focused on untimely payments, tracking of improper payments and segregation of duties; there were no controls identified for invalid payments. No additional risks were identified by PNNL related to improper/invalid payments. **Sources: D2, D5, D10, D22, D23, I7, I14**	RC
A4	Are policies based on technical information?	In the past, PNNL events were centered on internal fraudulent activities. The focuses of the internal controls were written to prevent or detect internal fraud. The AGs do not discuss awareness or detection/identification of potential external fraudulent activities in the Vendor Management Process. **Source: D6, D25, I12, I18**	
A5	Do policies conform to codes, standards, and regulations?	PNNL focuses efforts related to fraud identification and prevention on internal sources, such as segregation of duties, unethical behavior by employees, kickbacks to employees from subcontractors and vendors, etc. There are no specific requirements to identify, detect and prevent fraud by external entities; the requirements in OMB Circular A-123 are broad in nature. **Source: D12, D17, D18**	
A6	Are policies/implementing programs and procedures in place at all organization levels?	High level policies do not address external criminal fraud in the Vendor Management Process. Lower-level desk guides were not adequate to detect or mitigate external fraud. **Source: D2, D9,D10, D12, D17, D18**	RC
A7	Are policies consistent at all organization levels?		
A8	Are policies clear and understandable?	High level policies do not address the potential for external fraud in the Vendor Management Process. **Source: D2, I4, I9, I11**	
A9	Are policies implementable?	Yes.	

A10	Are policies applicable to all areas of operation?	No. There were no policies around external fraudulent activities. **Source: I13-15, I16, I18**	
A11	Are policies congruent with organization goals?		

A – Management System Factors			
MA2	Implementation LTA	Does the overall management program actually represent the intent of the policy statement? Are problems encountered during the conduct of work relayed back to the policy makers? Is policy implementation a balanced effort with focus on personnel, procedures, and plant equipment? Is the implementation generally pro-active?	
Conclusion: BSD Management did not clearly define adequate controls regarding the identification, detection and response to potential fraudulent activities by external entities in the Vendor Management Process. High level policies and procedures, such as the Acquisition Guidelines do no address expectations for fraudulent activities with respect to the Vendor Management Process. Previous issues surrounding fraudulent activities stemmed from internal problems focusing EOD and self-assessments on looking at measures to keep internal fraudulent activities from occurring. Policies and requirements that were followed focused on internal threats.			
Section #	**Title**	**Causal Factors/Observations**	**Cause Ref**
A1	Are appropriate methods used for implementing/ improving personnel performance?	On the job training was given to the AP vendor coordinator by the previous Acquisition Coordinator and AP Manager. The training was informal and contained "tribal knowledge" of processes and expectations. **Source: D2, I4, I9, I11**	
A2	Line Responsibility: Is there a clear written statement of responsibility within the line organization?	Ownership of the Vendor Management Process resides within the Acquisitions M&O Program. Through EOD, the Vendor Management Process Desk Guide states that "the Accounts Payable manager is responsible for the oversight of the vendor process, which includes any changes to policy." Confusion on who actually has ownership of the process. **Source: D2, D15, D20, I2, I7, I14-15,**	

A3	Are appropriate staff responsibilities identified?	R2A2s not written for key staff. Previous AP Manager used to execute ACH changes, the new AP Manager does not. Previous Contracts Vendor Coordinator executed ACH changes, now the AP Vendor Coordinator performs this duty. The task was given to her when the hired replacement Contracts Vendor Coordinator left PNNL shortly after she started. **Sources: I7, I14-15, D24**	
A4	Has management identified and specified the types of information it needs?	The EOD and self-assessments did not look at external fraudulent information. The focus was internal fraud and performance. **Source: D22-23**	
A5	Is there a clear written directive disseminated throughout the organization?	Expectations for what is required in the organization is understood, but the controls needed were not implemented. The goal is customer support and assurance the Lab meets payment requirements.	
A6 [E]	Has top level management provided the type of support needed by those lower in the organization?	Top level management meets with direct managers on a frequent basis to discuss organizational needs/issues. The expectation is for management to flow down information to support staff.	
A7	Is the department budget adequate?		
A8	Are there unnecessary delays in implementing program elements?		
A9	Is line management held accountable for implementation?		
A10	Does top level management show a high interest by personal involvement at low levels of the organization?		

A – Management System Factors		
MB4	Program Review LTA	Does the program under review provide for low cost, high production services, professional growth, clear career path, and the use of state of the art methods? Is there a means provided to measure the effectiveness of the program?

Conclusion: In the absence of the appropriate controls, training and staff transitions play an important component in fraud detection which both were lacking. Training of key roles was done informally and as a hands- on type of activity with no training guide. Transition of at least three key staff occurred, resulting in a loss of knowledge and experience.

Section #	Title	Causal Factors/Observations	Cause Ref
a1	Is there adequate policy statement which summarized the ideas of the program? Do these policies provide a means for measuring the program's success and improvements?	Upper-level policies/procedures do not contain clearly defined controls regarding identification, detection and response to potential fraud from external sources in relation to the Vendor Management Process. Requirements from OMB A-123 are broad in nature and do not explicitly address fraud from external sources. Self-assessments are performed by the organization but do not look at fraud from external sources. **Source: D9,D10**	
a2	Are there operating manuals, job descriptions, or appropriate schematics for the program? Are operating data available and evaluated?	The controls for the Vendor Management Process in processing ACH banking changes were not adequate to detect a fraudulent request. The Vendor Management Process Desk Guide was developed by the Contracts and AP Vendor Coordinators as a "How to" document. **Source: D2, I7**	DC
a3	Is there a formal measurement system which compares job performance with program ideals and objectives?	Self-assessments are performed evaluating execution of functions and requirement. However, assessments related to the identification, detection and prevention of external fraud are not included. **Source: D22-23**	

a4	Does the program have an adequate organization specified?		
b1	Are there appropriately trained technical and managerial personnel within the program? Is their status appropriate for their position within the organization? Are they qualified on the basis of education and experience?	There are trained staff and managers in the organization. However, some R2A2s are unclear and staff turnover in key positions has resulted in loss of knowledge and experience. The prior management and staff were not specifically looking for external fraud; the desk guide contained limited controls for external fraudulent activities in the Vendor Management Process. **Source: I4, I7, I9, I11**	RC
b2	Where necessary, are there appropriate, on-going committees and project task forces used to improve the functioning of the program? Do these groups take a realistic view of the problems encountered?	There is no program within BSD that is responsible for monitoring external information sources (e.g., FBI website) for the existence of potential threats or scams perpetrated by external entities. There is no routine monitoring of emerging scams or threats from external sources. SMEs are typically tasked with the responsibility for monitoring external requirements changes and keeping informed about their technical area for an M&O program. BSD relies on individual staff members to identify and respond to potential fraudulent activity by external sources; however, this is not a written expectation.	RC
b3	Does the scope of the program cover all potential problem areas likely to be encountered? Does this program utilized advance technical R&D?	No policy was developed for external fraudulent activities. Until recently (late 2015), previous fraudulent issues that have occurred at PNNL have been internal in nature. A more current fraud activity involves using the name of the current Procurement Director to request quotes for consumer electronics from vendors, setting up a Purchase order and receiving goods at the fraudulent entity's specified address without pre-payment. PNNL's response focused on whether or not false invoices would be detected and paid to the fraudulent entity. **Source: D2, D6, D22-23, I2, I7, I14-18**	RC

b4	Is the program properly integrated with the other programs within the organization?	Ownership of the Vendor Management Process resides within the Acquisitions M&O Program. The Vendor Management Process Desk Guide states that "the Accounts Payable manager is responsible for the oversight of the vendor process, which includes any changes to policy." Through interviews in both groups, there was confusion regarding integration of Vendor Management Process functions between Contracts and AP, and which organization was actually responsible for policy and oversight. **Source D2, D15, D20, I2, I7, I14-15**	
b5	Is the program organized to achieve continuous improvement through data collection, analysis, and feedback?		

Appendix E. Hazard-Barrier-Target Analysis

Problem Statement: An invoice payment was believed to have been made to the bank account of a PNNL subcontractor on December 16, 2016. On January 12, 2017, it was subsequently discovered that the payment had incorrectly been made to a bank account for a fraudulent entity posing as a legitimate subcontractor that was set up in the PNNL Vendor Master File.

Hazard: Payment to external fraudulent entities through the Vendor Management Process

Target: BSD Controls/Polices for the Vendor Management Process

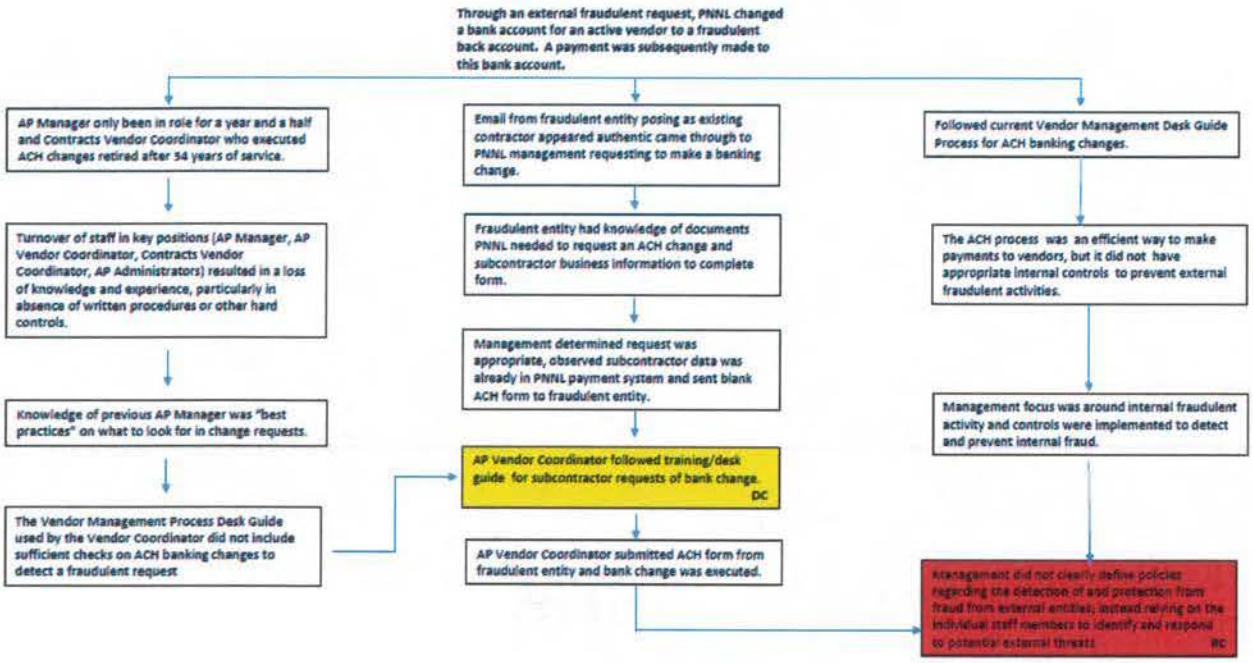
Advertised Barriers	Did Not Provide	Did Not Use	LTA/ Failed	Did Not Fail	Comment	Cause Reference
Key Roles within AP AP/Acquisitions Training			X		On the job training was given to the AP Vendor Coordinator by the previous Contracts Vendor Coordinator and AP Manager. The training was informal and included "tribal knowledge" of processes and expectations. Training given to the current AP Manager during the transition from the previous manager was abbreviated.	
AP Desk Guide				X	AP Desk Guide includes a review of banking information against the information in the Vendor Master File when vouchering and paying an invoice. AP Desk Guide does not cover the ACH bank change request process; this is covered in the Vendor Management Process Desk Guide.	
Vendor Management Process Desk Guide			X		AP Vendor Coordinator validated the ACH bank change request in accordance with the training and Vendor Management Desk Guide which only required confirmation of the address and SSN# or Tax ID# to what was currently on file. The desk guide was inadequate and lacked the necessary controls to detect external	Direct Cause

Advertised Barriers	Did Not Provide	Did Not Use	LTA/ Failed	Did Not Fail	Comment	Cause Reference
					criminal fraud due to the current sophistication of the fraud environment.	
People - AP Manager			X		The AP Manager received the ACH bank change request via an email from the Procurement Director. The request appeared to come from a known vendor which PNNL had been doing business with for the past 10 years. The AP Manager confirmed the information provided but did not identify the banking request as from a fraudulent entity. The AP Manager forwarded the completed ACH bank change form to the AP Vendor Coordinator to make the requested changes.	
People - AP Vendor Coordinator			X		The AP Vendor Coordinator received the completed ACH form via email from the AP Manager. The AP Vendor Coordinator followed procedures as described in the Vendor Management Process Desk Guide. The desk guide lacked the necessary controls to detect this type of fraud.	Direct Cause
Purchase Expense System (PES)				X	PES was used to update the vendor bank account information as intended.	
BSD Policies / Procedures			X		There were no upper-level policies or procedures (including the PNNL AGs) that covered identification, detection and response to potential fraud from external criminal entities in the Vendor	Root Cause

Advertised Barriers	Did Not Provide	Did Not Use	LTA/ Failed	Did Not Fail	Comment	Cause Reference
					Management Process.	
PNNL A-123 controls for AP (C399, C428, C435)			X		DOE provided risk statements in the AP process area (CR2301 and CR2309) that covered improper, invalid or untimely updates to the Vendor Master File and improper, invalid or untimely payments. PNNL's mitigating controls identified for these risk statements (C399, C428 and C435) focused on untimely payments, tracking of improper payments and segregation of duties, and not on invalid payments (e.g., payments to fraudulent subcontractors).	Root cause

Conclusion: Analysis of the barriers listed above indicates that there were no upper-level policies or procedures addressing the identification, detection and response to fraud from external criminal entities. Flow down of this information to documents such as the as the Vendor Management Desk Guide did not include controls for the detection and mitigation of external fraudulent activity. Mitigating controls for DOE-provided risk statements in the AP process area focused on untimely payments, tracking of improper payments and segregation of duties. There was no mitigating control that focused on invalid payments (e.g., payments to fraudulent entities).

Appendix E. Why Tree Analysis



Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by **Battelle** *Since 1965*

U.S. DEPARTMENT OF
ENERGY

902 Battelle Boulevard
P.O. Box 999
Richland, WA 99352
1-888-375-PNNL (7665)

www.pnnl.gov

Approval History for: E-01159 Payment to a Fraudulent Subcontractor CA

Final Process State: APPROVED

Name		Activity Name	Date
☒ ACCEPTED	Pryor, Kathryn H	Approval	4/24/2017 1:32:21 PM
☒ ACCEPTED	Anderson, Stephanie J	Approval	4/24/2017 1:36:03 PM
☒ ACCEPTED	Mendoza, Donaldo P	Approval	4/26/2017 7:16:50 AM
☒ ACCEPTED	Anderson, Iris E	Approval	5/1/2017 1:02:27 PM

*** All actions are stored digitally and viewable at https://approvals.pnl.gov/ProcessView.aspx?pid=2697670**