U.S. ENVIRONMENTAL PROTECTION AGENCY

OFFICE OF INSPECTOR GENERAL

Information Technology

EPA Lacks Processes to Validate Whether Contractors Receive Specialized Role-Based Training for Network and Data Protection

Report No. 17-P-0344 **July 31, 2017**

Report Contributors:

Rudolph M. Brevard
Vincent Campbell
Eric K. Jackson, Jr.
Scott Sammons

Abbreviations

CIO	Chief Information Officer
COR	Contracting Officer's Representative
COTR	Contracting Officer Technical Representative
EPA	U.S. Environmental Protection Agency
FISMA	Federal Information Security Modernization Act
FY	Fiscal Year
IT	Information Technology
OAM	Office of Acquisition Management
OARM	Office of Administration and Resources Management
OEI	Office of Environmental Information
OIG	Office of Inspector General
OMB	Office of Management and Budget

Cover photos: OIG-created photo collage compiled from EPA photos.

Are you aware of fraud, waste or abuse in an EPA program?

EPA Inspector General Hotline
1200 Pennsylvania Avenue, NW (2431T)
Washington, DC 20460
(888) 546-8740
(202) 566-2599 (fax)
OIG_Hotline@epa.gov

Learn more about our OIG Hotline.

EPA Office of Inspector General
1200 Pennsylvania Avenue, NW (2410T)
Washington, DC 20460
(202) 566-2391
www.epa.gov/oig

Subscribe to our Email Updates
Follow us on Twitter @EPAoig
Send us your Project Suggestions

U.S. Environmental Protection Agency
Office of Inspector General

17-P-0344
July 31, 2017

At a Glance

Why We Did This Review

The U.S. Environmental Protection Agency (EPA), Office of Inspector General (OIG), conducted this audit to determine what processes the EPA uses to verify that agency contractors with significant information system security responsibilities meet established specialized training duties.

Role-based training is continuous education that improves current knowledge, skills and abilities for particular job functions. Under the Chief Information Officer's Federal Information Security Modernization Act (FISMA) Metrics, agencies are responsible for identifying and reporting specialized security training, such as role-based training, for all personnel (including contractors) with significant information security responsibilities.

This report addresses the following EPA goal or cross-agency strategy:

- *Embracing EPA as a high-performing organization.*

Send all inquiries to our public affairs office at (202) 566-2391 or visit www.epa.gov/oig.

Listing of OIG reports.

EPA Lacks Processes to Validate Whether Contractors Receive Specialized Role-Based Training for Network and Data Protection

What We Found

The EPA is unaware of the number of agency contractors who have significant information security responsibilities and require role-based training. This is attributed to the following factors:

- EPA personnel overseeing contractors are not aware of contractor role-based training requirements.
- The agency has not included role-based training requirements in all awarded contracts.
- The EPA lacks a process to track and report contractors' role-based training.

The EPA is unaware whether information security contractors possess the skills and training needed to protect the agency's information, data and network from security breaches.

In addition, the EPA did not report contractor training status in its fiscal years 2015 and 2016 Chief Information Officer's Annual FISMA reports submitted to the Office of Management and Budget. FISMA guidance requires agencies to train and oversee personnel (including contractors) who have significant responsibilities for information security, and report on the effectiveness of the information security program.

Insufficient awareness, contract requirements, and oversight of role-based training increase the risk that EPA contractors may lack the knowledge or skills necessary to protect the agency from cyberattacks. The agency also has insufficient information to manage risks to its data and network.

Recommendations and Planned Agency Corrective Actions

We recommend that the Assistant Administrator for Administration and Resources Management update the EPA Acquisition Guide to include the newly developed cybersecurity contract clauses that agency personnel must include in all EPA contracts, and include the cybersecurity contract clauses in all existing and future information technology contracts. We also recommend that the Office of Environmental Information implement a process for agency personnel to maintain a listing of contractor personnel required to take role-based training and report this information in the Chief Information Officer's Annual FISMA reports. The agency concurred with our recommendations and provided planned corrective actions with estimated completion dates. One recommendation has been resolved with corrective action completed. All remaining recommendations are resolved with corrective actions pending.

UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
WASHINGTON, D.C. 20460

THE INSPECTOR GENERAL

July 31, 2017

MEMORANDUM

SUBJECT: EPA Lacks Processes to Validate Whether Contractors Receive Specialized Role-Based Training for Network and Data Protection
Report No. 17-P-0344

FROM: Arthur A. Elkins Jr.

TO: Steven Fine, Acting Assistant Administrator and Chief Information Officer
Office of Environmental Information

Donna J. Vizian, Acting Assistant Administrator
Office of Administration and Resources Management

This is our report on the subject audit conducted by the Office of Inspector General (OIG) of the U.S. Environmental Protection Agency (EPA). The project number for this audit was OA-FY16-0104. This report contains findings that describe the problems the OIG has identified and corrective actions the OIG recommends. This report represents the opinion of the OIG and does not necessarily represent the final EPA position.

Action Required

You are not required to provide a written response to this final report. We consider all recommendations resolved. Should you choose to provide a final response, we will post your response on the OIG's public website, along with our memorandum commenting on your response. Your response should be provided as an Adobe PDF file that complies with the accessibility requirements of Section 508 of the Rehabilitation Act of 1973, as amended. The final response should not contain data that you do not want to be released to the public; if your response contains such data, you should identify the data for redaction or removal along with corresponding justification.

We will post this report to our website at www.epa.gov/oig.

Table of Contents

Appendices

Purpose

The Office of Inspector General (OIG) for the U.S. Environmental Protection Agency (EPA) conducted this audit to determine what processes the EPA uses to verify that agency contractors with significant information system security responsibilities meet established specialized training requirements.

Background

Under the Chief Information Officer's Federal Information Security Modernization Act (FISMA) Metrics, agencies are responsible for identifying and reporting specialized security training, such as role-based training, for all personnel (including contractors) with significant information security responsibilities.

Role-based training is role-specific training for an individual based on their functional job and responsibilities.

System administrators and network engineers are examples of positions that require an individual to perform significant information security responsibilities. Role-based training for a system administrator may include tutorials on performing configuration changes on an application or system, or reviewing system logs to detect suspicious activity. Role-based training for a network engineer may include tutorials on establishing firewall rules, or that highlight the consequences of not implementing security controls.

On March 10, 2016, the EPA had obligated $546,470,844 for 688 information technology (IT) contract task orders. These IT contracts include various operational IT and telecommunication services, as well as IT equipment. Many of the positions included in these contracts require contractors to perform duties requiring specialized training.

Responsible Offices

The Office of Information Security and Privacy, within the Office of Environmental Information, is responsible for managing the EPA's information security training program. This office is also responsible for tracking and reporting the training status of personnel (including contract employees) who have significant information security responsibilities and are required to take role-based training. The Office of Acquisition Management, within the Office of Administration and Resources Management, is responsible for planning and administering contracts for the agency. Contracting Officer's Representatives (CORs) and Contracting Officer Technical Representatives (COTRs) from all EPA offices are responsible for monitoring contracts to verify that all requirements are being met.

Federal and EPA Guidance

Office of Management and Budget (OMB) Circular No. A-130, *Managing Information as a Strategic Resource,* Appendix I, requires agencies to provide role-based training to employees and contractors who perform assigned security duties.

The U.S. Department of Homeland Security's Chief Information Officer's FISMA Metrics require federal agencies to annually report the number of network users and other staff who have significant information security responsibilities and successfully completed role-based training.

The EPA's guidance is outlined in Chief Information Officer (CIO) 2150-P-02.2, *Information Security–Awareness and Training Procedures*, which was approved February 16, 2016. Provisions pertaining to role-based security training include the following requirements:

- EPA personnel, contractors or others working on behalf of the EPA, and who have significant security responsibilities shall receive initial specialized training and annual refresher training specific to their security responsibilities.

- Service managers, in coordination with EPA officers and officials, shall verify that service providers develop and maintain role-based training, education and credentialing requirements to confirm that "contractors designated as having significant information security responsibilities receive adequate training with respect to such responsibilities."

- EPA Information Security Officers shall "identify all individuals requiring role-based security-related training within their respective program offices or regions."

- "Training or instruction for contractors should be identified or described" in the statement of work or the performance work statement.

Scope and Methodology

We performed our audit from March 2016 through April 2017. We conducted this performance audit 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 reviewed federal and EPA criteria related to our objective. We assessed a judgmentally selected sample of five IT contracts from the EPA's 688 IT contracts valued at approximately $546.5 million on March 10, 2016. Table 1 shows the five IT contracts we reviewed, which are valued at $165.6 million.

Sixty-nine (10 percent) of the EPA's 688 IT contract task orders are each greater than $1 million. The 69 contracts also make up 92 percent ($500.5 million) of all monies obligated for IT contracts.

Table 1: EPA contracts reviewed

Contract number	Responsible office	Purpose	Amount
1	Office of Environmental Information	Custom application management contract at the EPA's National Computer Center	$71,148,530
2	Office of Environmental Information	IT hosting services at the EPA's National Computer Center	$45,917,563
3	Office of Environmental Information	General IT contract for active directory services, desktop applications, security partitioning, remote access and other services	$36,284,637
4	Office of Administration and Resources Management	Operation and maintenance support for the EPA Acquisition System	$8,054,699
5	EPA Region 6	IT service and support for EPA Region 6	$4,207,700
Value of contract task orders reviewed			$165.6 million

Source: EPA-compiled data.

We also performed the following activities:

- Determined whether the contract language requires contractors with significant information system security responsibilities to complete specialized role-based training on a periodic basis.
- Interviewed CORs and a COTR to obtain additional information on the requirement for roles and duties of the contractors, and whether those contractors should have completed specialized role-based training for individuals with significant information security responsibilities.
- Interviewed EPA management responsible for tracking and reporting the training status of EPA employees and contractors who have significant information security responsibilities, and are required to complete specialized role-based training.

There were no prior audit recommendations for the OIG to do follow-up.

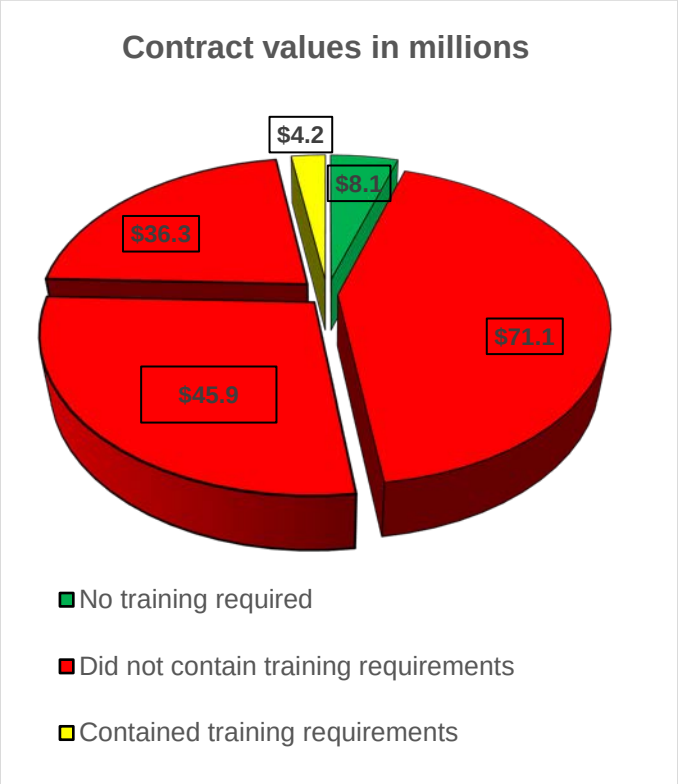
Results of Audit

The EPA is unaware of the number of contractors who have significant information security responsibilities and require role-based training. As noted in Figure 1, our analysis of the five reviewed IT contracts valued at $165.6 million disclosed that four of the five reviewed contracts had contractor personnel who performed duties with significant information security responsibilities and were required to complete role-based training.

Only one of the four contracts with contractor personnel who had significant information security responsibilities contained language requiring those individuals to complete role-based training. That contract was valued at $4.2 million. The remaining three contracts (valued at $153.4 million) did not contain such language.

Furthermore, the EPA did not report contractor training status in its fiscal year (FY) 2015 CIO Annual FISMA Report submitted to OMB. During our FY 2016 FISMA audit, we confirmed the agency still had not collected or reported data for FY 2016.

Figure 1: Analysis of five IT contracts reviewed for role-based training requirements



Source: Information compiled by the EPA OIG.

Federal law and EPA guidance require employees and contractors to complete role-based training. FISMA requires agencies to train and oversee personnel (including contractors) with significant responsibilities for information security, and to report to the agency head on the effectiveness of the information security program. FY 2015 and FY 2016 CIO FISMA Metrics issued by the U.S. Department of Homeland Security required federal agencies to report to OMB the number of network users and other staff who have significant information security responsibilities. Agencies were also required to report the number of users who have successfully completed role-based training.

The EPA lacks internal controls to know how many contractors require role-based training. In part, this is attributed to the following:

- EPA personnel overseeing contractors are not aware of contractor role-based training requirements.
- The agency has not included role-based training requirements in all awarded contracts.
- The EPA has not implemented an oversight process to track and report contractor compliance with role-based training.

As a result, EPA management lacks the necessary data to make risk-based decisions about the capabilities of its contractor workforce charged with protecting the confidentiality, integrity and availability of the agency's network and data.

EPA Does Not Monitor Contract Personnel Who Have Significant Information Security Responsibilities

The agency's CORs are responsible for managing four of the five sampled IT contracts, but they could not accurately identify the number of contractor employees associated with the contracts and task orders, or individuals who have significant information security responsibilities. Three CORs stated that to their knowledge, contractors performing significant information security duties on those contracts are not completing the required annual role-based training. One of these CORs was unaware that role-based training was required for contractors who have significant information security responsibilities. This COR believed the training was only required for federal employees. Only one COTR ensured that contract personnel completed role-based training.

The EPA Acquisition Guide provides the agency with guidance for acquiring goods and services. Our review of this guidance found that it lacks requirements related to tracking, monitoring and reporting on the status of contractors with significant information security responsibilities who have completed required specialized training.

We also contacted Information Security Officers from two EPA program offices. Information Security Officers are responsible for identifying contract personnel required to take role-based training, and we asked the officers what steps EPA program offices took to verify contractors completed the required training. Information Security Officers indicated that role-based training is targeted to federal employees. According to the officers, they do not track contractors, even though officers are required to identify ***all individuals*** requiring role-based security-related training within their respective program offices or regions as prescribed in CIO 2150-P-02.2, *Information Security–Awareness and Training Procedures.*

After the release of our draft report, Office of Acquisition Management (OAM) officials indicated that they developed Interim Policy Notice # 17-01, *Use of 22 Cybersecurity Tasks*, which identifies 22 cybersecurity tasks that are to be included in existing and new performance work statements and statements of work. One cybersecurity task requires the contractor to ensure that contractor personnel with significant information security responsibilities complete specialized information security training based on the requirements defined in the EPA's role-based training program.

EPA Has Not Consistently Included Requirements for Contract Personnel to Complete Role-Based Training

We learned from an EPA official that, as of the beginning of FY 2017, the agency has developed standard information security contract clauses to require contractors to comply with federal and EPA information security requirements, including requirements to complete role-based training. The EPA official stated that the agency is in the process of reviewing all new FY 2017 contracts to verify that new contracts contain the clauses. However, the official said no milestone dates have been established to review existing contracts for the inclusion of the clauses.

Our analysis revealed that four of the five IT contracts in our sample included positions requiring an individual to perform significant information security responsibilities, such as system administrators and privileged users. As noted in Figure 1, only one of the four contracts contained language requiring contractors to complete role-based training.

In December 2016, OAM officials indicated that they developed Interim Policy Notice # 17-01. The policy states that the EPA's Office of Environmental Information (OEI) is responsible for including any of the 22 subject tasks as necessary in its new statements of work and performance work statements. OEI must also coordinate with OAM to process any necessary resultant contract/solicitation modifications or amendments that OAM makes. The policy further states that CORs who do not work in OEI should seek assistance from OEI when choosing which, if any, of the 22 subject tasks must be added or included in the COR's performance work statement or statement of work.

In June 2017, OEI notified EPA program and regional offices that any offices requesting IT products or services would have to complete a checklist that includes the 22 cybersecurity tasks when submitting procurement requests. OEI further indicated that after June 30, 2017, OAM will no longer accept any procurement requests that do not include this checklist.

EPA Has Not Implemented an Oversight Process to Track and Report Contractor Compliance With Role-Based Training

OEI is responsible for overseeing the agency's information security program, but the office is not aware of the status of contractors who have completed role-based training because the office has not established a process to track and report this data. CIO 2150-P-02.2, *Information Security–Awareness and Training Procedures* requires the CIO to ensure that role-based security training is completed by agency personnel, and that effective tracking and reporting mechanisms are in place.

An EPA official indicated that currently the agency only tracks and reports information on whether EPA federal employees with significant information security responsibilities have completed role-based training. The EPA official stated that there were no plans to track and report the status of role-based training for contractors because the agency was unaware of any requirement to report this as part of its CIO FISMA data submission to OMB.

The agency official indicated that CIO FISMA Metrics did not specifically require reporting this data for contract employees. However, our review of the FY 2016 CIO FISMA Metrics revealed that personnel with significant information security responsibilities is defined in the following manner: "Those with significant security responsibilities include administrators and users with privileged network accounts and those that affect security."

The FY 2016 CIO FISMA Metrics contain the following definition of a privileged network:

> A network account with elevated privileges, which is typically allocated to system administrators, network administrators, and others who are responsible for system/application control, monitoring, or administration functions.

Our analysis revealed that four of the five sampled IT contracts contained positions that require an individual to perform significant information security responsibilities, such as system administrators and privileged users. Given that these contractors have system access that would enable them to bypass security controls designed to detect malicious or suspicious activities on EPA systems, the agency should have included contractors with privilege accounts in its FISMA data reported to OMB.

Conclusion

Periodic role-based training provides the EPA with a mechanism to enhance the technical knowledge and skills of its workforce, who perform significant information security duties. These duties help to protect the EPA's security

infrastructure for environmental applications, including those applications developed and managed by contractors. Without consistently developing contractor employees' specialized skills in positions to combat ever-increasing cyberattacks, EPA applications are more likely to be compromised by a security breach where personally identifiable and other information could be lost or altered. This could lead to compromised identities, or the potential for environmental data used to protect and improve human health and the environment being altered or erased.

By not tracking and reporting the training status of contractors with significant information security responsibilities, the EPA does not have an accurate assessment of its information security workforce, and cannot accurately plan and budget for remediating security risks.

Recommendations

We recommend that the Assistant Administrator for Administration and Resources Management:

1. Update the EPA Acquisition Guide to include cybersecurity tasks contained in Interim Policy Notice # 17-01, *Use of 22 Cybersecurity Tasks* (December 2016).

2. Develop and implement a strategy to include the information security contract clause requiring contractors to complete role-based training into all existing and future information technology contracts and task orders.

We recommend that the Assistant Administrator for Environmental Information and Chief Information Officer:

3. Work with the Assistant Administrator for Administration and Resources Management to implement a process that requires appropriate agency personnel to maintain a listing of contractor personnel who have significant information security responsibilities and are required to take role-based training. This process should require appropriate agency personnel to validate and report to the Chief Information Security Officer that all relevant contractor personnel have completed role-based training.

4. Include the number of contractors who have significant information security responsibilities and have completed the required role-based training in the Chief Information Officer's Annual Federal Information Security Modernization Act reports submitted to the Office of Management and Budget.

Agency's Response and OIG Evaluation

The EPA's Office of Administration and Resources Management disagreed that it should implement Recommendation 1, and indicated that OEI should be responsible for implementing the recommendation. However, EPA policy places responsibility for the acquisition process with OAM. We noted that after the release of our draft report, OAM developed a new interim policy that identified 22 cybersecurity tasks that agency personnel must be aware of and include in all agency contracts. As such, we revised Recommendation 1 to request that the Office of Administration and Resources Management update the EPA Acquisition Guide to include the interim policy. OAM concurred with the revised Recommendation 1 and provided a planned corrective action with a milestone date of October 31, 2019. Recommendation 1 is resolved pending completion of the corrective plan.

OAM agreed with Recommendation 2 and further indicated that it has developed an interim policy that contains tasks for the contractor to complete to ensure that contractor personnel with significant information security responsibilities complete specialized information security training based on the requirements defined in the EPA role-based training program. OEI further distributed these cybersecurity tasks to agency officials. OEI provided a planned corrective action with a milestone date of June 30, 2017 for Recommendation 2. The recommendation is resolved and closed with corrective action completed.

OEI disagreed, in part, with Recommendation 3. The agency indicated that additional personnel outside of OEI have responsibility for tracking and validating whether contractors with significant information security have completed role-based training. OEI agreed that it should develop a process to confirm all required training has been performed. We noted that EPA policy holds the CIO responsible for ensuring the completion of role-based security training, and for ensuring that tracking and reporting mechanisms are in place. While the CIO may collaborate with other EPA offices, the CIO remains ultimately responsible for executing these functions. We revised Recommendation 3 to include language that states appropriate agency personnel should maintain a listing of contractor personnel who have significant information security responsibilities required to take role-based training, and to validate and report this information to the Senior Agency Information Security Officer.

The agency requested that we further revise Recommendation 3 to include working with the Office of Administration and Resources Management to develop this process, and that the information derived from this new process should be reported directly to the Chief Information Security Officer. As such, we revised Recommendation 3 to incorporate the suggested language. OEI provided a planned corrective action with a milestone date of December 31, 2018. Recommendation 3 is resolved pending completion of the corrective plan.

OEI agreed with Recommendation 4 and provided a planned corrective action with a milestone date of September 30, 2017. Recommendation 4 is resolved pending completion of the corrective plan.

Status of Recommendations and Potential Monetary Benefits

RECOMMENDATIONS

Rec. No.	Page No.	Subject	Status[1]	Action Official	Planned Completion Date	Potential Monetary Benefits (in $000s)
1	8	Update the EPA Acquisition Guide to include cybersecurity tasks contained in Interim Policy Notice # 17-01, *Use of 22 Cybersecurity Tasks* (December 2016).	R	Assistant Administrator for Administration and Resources Management	10/31/19	
2	8	Develop and implement a strategy to include the information security contract clause requiring contractors to complete role-based training into all existing and future information technology contracts and task orders.	C	Assistant Administrator for Administration and Resources Management	6/30/17	
3	8	Work with the Assistant Administrator for Administration and Resources Management to implement a process that requires appropriate agency personnel to maintain a listing of contractor personnel who have significant information security responsibilities and are required to take role-based training. This process should require appropriate agency personnel to validate and report to the Chief Information Security Officer that all relevant contractor personnel have completed role-based training.	R	Assistant Administrator for Environmental Information and Chief Information Officer	12/31/18	
4	8	Include the number of contractors who have significant information security responsibilities and have completed the required role-based training in the Chief Information Officer's Annual Federal Information Security Modernization Act reports submitted to the Office of Management and Budget.	R	Assistant Administrator for Environmental Information and Chief Information Officer	9/30/17	

[1] C = Corrective action completed.
R = Recommendation resolved with corrective actions pending.
U = Recommendation unresolved with resolution efforts in progress.

Appendix A

UNITED STATES ENVIRONMENTAL PROTECTION AGENCY

WASHINGTON, D.C. 20460

OFFICE OF
ADMINISTRATION
AND RESOURCES
MANAGEMENT

[May 18, 2017]

OARM's Response to Draft Report Recommendations

MEMORANDUM

SUBJECT: Response to Office of Inspector General Draft Report No. OA-FY16-0104, "*EPA Does Not Track Contractors Required to Take Role-Based Training*," dated April 19, 2017

FROM: Donna Vizian, Acting Assistant Administrator

TO: Arthur A. Elkins, Jr., Inspector General
Office of Inspector General

Thank you for the opportunity to respond to the issues and recommendations in the subject audit report. Following is a summary of the Office of Administration and Resources Management's overall position, along with its position on each of the report recommendations to the OARM.

OARM'S OVERALL POSITION:

Overall, the agency concurs with the findings and recommendations of this report.

OARM's RESPONSE TO REPORT RECOMMENDATIONS #1 AND #2:

Agreements

No.	Recommendation	Agency Explanation/Response	Completion Date
1	Require contracting officer's representatives and contracting officer technical	The EPA's Chief Information Officer 2150-P-02.2, Information Security–	12/31/2017

No.	Recommendation	Agency Explanation/Response	Completion Date
	representatives to confirm that contractors who have significant information security responsibilities have completed the required role-based training in accordance with federal and EPA policy and procedures.	Awareness and Training Procedures, in addressing role-based security training for all information systems state: *" The SAISO, in coordination with SOs, ISOs, IMOs, IOs, Managers and Supervisors, for EPA-operated systems, shall; and SMs, in coordination with the SAISO, IOs, ISOs and IMOs, for systems operated on behalf of the EPA, shall ensure service providers: Develop and maintain role based training, education and credentialing requirements to ensure EPA employees and contractors designated as having significant information security responsibilities receive adequate training with respect to such responsibilities."* It appears that the Office of Environmental Information would have the primary role in the implementing this recommendation. To the extent it is determined that the EPA, under any given contract and as identified by the program or technical requisitioner, requires that contractor personnel with elevated access must be provided specialized security training, such as role-based training, and that such requirement is identified or described in the contract statement of work or performance work statement, the Office of Administration and Resources Management/Office of Acquisition Management will require the contracting officer's representative (which include	

No.	Recommendation	Agency Explanation/Response	Completion Date
		contracting officer's technical representative) to confirm that contractor personnel who have significant information security responsibilities have completed the required role-based training in accordance with federal and EPA policy and procedures. It is contemplated that this confirmation will be obtained from the COR periodically, and no less than annually. The OARM/OAM will also ensure that the CORs appointment memorandum for contract CORs where such a requirement is present in the contract, explicitly include the responsibility to monitor and report on the required completion of role-based training by contractor personnel.	
2	Develop a strategy to include the information security contract clause requiring contractors to complete role-based training into all existing and future information technology contracts and task orders.	The OARM/OAM concurs with the development of a strategy to include the proper clause(s) in existing and future contracts, not just IT contracts, but all contracts to which this would apply. For example, a mission support contract under which some IT services are provided may need to have the clauses also. The OARM/OAM will collaborate with the OEI and other agency personnel with IT expertise in the development of this strategy.	12/31/2017

No.	Recommendation	Agency Explanation/Response	Completion Date

CONTACT INFORMATION. If you have any questions regarding this response, please contact Celia Vaughn, Chief of Staff, Office of Acquisition Management, at 202-564-1047.

Appendix B

UNITED STATES ENVIRONMENTAL PROTECTION AGENCY

WASHINGTON, D.C. 20460

OFFICE OF
ADMINISTRATION
AND RESOURCES
MANAGEMENT

[June 19, 2017]

OARM's Updated High-Level Corrective Action Plan

High-Level Corrective Action Plan as of June 19, 2017:

OARM's RESPONSE TO REPORT RECOMMENDATIONS #1 AND #2:

No.	Recommendation	Agency Response	Revised Recommendation	Agency Response	Planned Milestone Date
1	Require contracting officer's representatives and contracting officer technical representatives to confirm that contractors who have significant information security responsibilities have completed the required role-based training in accordance with federal and EPA policy and procedures.	The EPA's Chief Information Officer 2150-P-02.2, Information Security–Awareness and Training Procedures, in addressing role-based security training for all information systems state: *" The SAISO, in coordination with SOs, ISOs, IMOs, IOs, Managers and Supervisors, for EPA-operated systems, shall; and SMs, in coordination with the SAISO, IOs, ISOs and IMOs, for systems operated on behalf of the EPA, shall ensure service providers: Develop and maintain role based training, education and*	Update the EPA's Acquisition Guide, to include the Interim Policy Notice # 17-01 Use of 22 Cybersecurity Tasks (December 2016)	OAM does not feel comfortable setting any date for this Interim Policy Notice (IPN) # 17-01 – Use of 22 Cybersecurity Tasks (December 2016), because this is really an OMB initiative. EPA, in being proactive, developed/prepared the IPN as official agency acquisition policy to be followed. With that said, an estimated milestone date would be October 31, 2019. This is contingent upon the:	October 31, 2019

No.	Recommendation	Agency Response	Revised Recommendation	Agency Response	Planned Milestone Date
		credentialing requirements to ensure EPA employees and contractors designated as having significant information security responsibilities receive adequate training with respect to such responsibilities." It appears that the Office of Environmental Information would have the primary role in the implementing this recommendation. To the extent it is determined that the EPA, under any given contract and as identified by the program or technical requisitioner, requires that contractor personnel with elevated access must be provided specialized security training, such as role-based training, and that such requirement is identified or described in the contract statement of work or performance work statement, the Office of Administration and Resources Management/Office of Acquisition Management will require the contracting officer's representative (which include contracting officer's technical representative) to confirm that contractor personnel who have significant information security responsibilities have completed the		1) use of the tasks in solicitations and the receipt of comments/feedback from the vendor communities; and/or 2) OMB's release of cybersecurity clauses via FAR (FAC-xx).	

No.	Recommendation	Agency Response	Revised Recommendation	Agency Response	Planned Milestone Date
		required role-based training in accordance with federal and EPA policy and procedures. It is contemplated that this confirmation will be obtained from the COR periodically, and no less than annually. The OARM/OAM will also ensure that the CORs appointment memorandum for contract CORs where such a requirement is present in the contract, explicitly include the responsibility to monitor and report on the required completion of role-based training by contractor personnel.			
2	Develop a strategy to include the information security contract clause requiring contractors to complete role-based training into all existing and future information technology contracts and task orders .	The OARM/OAM concurs with the development of a strategy to include the proper clause(s) in existing and future contracts, not just IT contracts, but all contracts to which this would apply. For example, a mission support contract under which some IT services are provided may need to have the clauses also. The OARM/OAM will collaborate with the OEI and other agency personnel with IT expertise in the development of this strategy.	Develop **and implement** a strategy to include the information security contract clause requiring contractors to complete role-based training into all existing and future information technology contracts and task orders	It is noted that OAM issued Interim Policy Notice (IPN) # 17-01 – Use of 22 Cybersecurity Tasks (December 2016) & addressed specialized information security training for staff with significant security responsibilities. https://oamintra.epa.gov/node/8?q=node/158 The IPN 17-01 established policy regarding the use of cybersecurity tasks and states:	06/30/2017

No.	Recommendation	Agency Response	Revised Recommendation	Agency Response	Planned Milestone Date
				"(a) In accordance with Deputy Director Cobert's guidance, the ***Offices of Environmental Information (OEI) and Acquisition Management (OAM) must collaborate*** *to provide expertise for recommending any contract changes or solicitation changes for new procurements, or any changes to existing PWSs or SOWs to incorporate the 22 subject cybersecurity tasks as necessary.* *(b)* ***OEI, as the Agency's cybersecurity technical experts, is responsible for including any of the 22 subject tasks as necessary in its new SOWs and PWSs, and coordinating with OAM*** *in processing any necessary resultant contract/solicitation modifications or amendments that OAM makes.* *(c)* ***Contracting Officer's Representatives (CORs) who do not work in OEI should seek assistance***	

No.	Recommendation	Agency Response	Revised Recommendation	Agency Response	Planned Milestone Date
				from OEI when choosing which if any of the subject 22 tasks must be added or included in the COR's PWS or SOW. *A COR may want to include an OEI representative as a cybersecurity consultant on the advanced procurement plan (APP) team for new requirements for information systems."* **Task H** - Specialized Information Security Training for Staff with Significant Security Responsibilities **addresses contractor requirements when tasked with such responsibilities** as follows: *"(a) The Contractor must ensure that Contractor personnel with significant information security responsibilities complete specialized information security training based on the requirements defined in the EPA role-based training program (program provided after Contract award).*	

No.	Recommendation	Agency Response	Revised Recommendation	Agency Response	Planned Milestone Date
				The objective of the information security role-based training is to develop an EPA information security workforce with a common understanding of the concepts, principles, and applications of information security to ensure the confidentiality, integrity and availability of EPA's information and information systems. The Contractor is required to report training completed to ensure competencies are addressed. The Contractor must ensure employee training hours are satisfied in accordance with EPA Security and Privacy Training Standards (provided after Contract award). The Contracting Officer's Representative (COR) will provide additional information for specialized information security training based on the requirements in paragraph (b). *(b) The following role-based*	

No.	Recommendation	Agency Response	Revised Recommendation	Agency Response	Planned Milestone Date
				requirements are provided: *[Program office adds role-based requirements; otherwise write "none" or "not applicable"]* *(c) The Contractor must ensure that all IT and Information Security personnel receive the necessary technical (for example, operating system, network, security management, and system administration) and security training to carry out their duties and maintain certifications.* *(d) The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder, provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer."* As confirmed by the OIG, corrective action is satisfied by the collaborative actions already taken by OAM and	

No.	Recommendation	Agency Response	Revised Recommendation	Agency Response	Planned Milestone Date
				OEI in developing, distributing and requiring the 22 Cybersecurity Tasks. Any contract changes or solicitation changes for new procurements, or any changes to existing PWSs or SOWs must incorporate the 22 subject cybersecurity tasks, **if any when applicable, and as necessary,** for procurement requests initiated after June 30, 2017.	

Appendix C

UNITED STATES ENVIRONMENTAL PROTECTION AGENCY

WASHINGTON, D.C. 20460

OFFICE OF
ENVIRONMENTAL
INFORMATION

[May 19, 2017]

OEI's Response to Draft Report Recommendations

MEMORANDUM

SUBJECT: Revised Response to Office of Inspector General Draft Report No. OA-FY16-0104 "*EPA Does Not Track Contractors Required to Take Role-Based Training,*" Dated April 19, 2017

FROM: Steven Fine,
Acting Chief Information Officer

TO: Arthur A. Elkins, Jr.
Inspector General

Thank you for the opportunity to respond to the issues and recommendations in the subject audit report. Following is a summary of the Office of Environmental Information's (OEI) overall position, along with its position on each of the report recommendations to OEI.

OEI'S OVERALL POSITION:

The agency agrees with the recommendations, with some points of clarification.

OEI'S RESPONSE TO REPORT RECOMMENDATIONS #3 AND #4:

No.	Recommendation	Agency Explanation/Response	Completion Date
3	Implement a process that requires appropriate Agency personnel to maintain a	OEI agrees with the revised recommendation, with a few clarifications. First, we would	12/31/2018

No.	Recommendation	Agency Explanation/Response	Completion Date
	listing of contractor personnel who have significant information security responsibilities required to take role-based training. This process should require appropriate Agency personnel to validate and report to the Senior Agency Information Security Officer that all relevant contractor personnel have completed role-based training.	ask that the recommendation be changed from "Implement a process" to state that "OEI will work with the Assistant Administrator for Administration and Resources Management to implement a process." This may require actions from Contracting Officer Representatives and would necessitate coordination with OARM. Second, OEI would attest that Agency personnel should respond to the Chief Information Security Officer, not the SAISO, that all relevant contractor personnel have completed role-based training.	
4	Include the number of contractors who have significant information security responsibilities and have completed the required role-based training in the EPA's Federal Information Security Modernization Act reports submitted to the Office of Management and Budget.	OEI agrees in part that based upon a recent change in A-130, Appendix I, this requirement can be met by the end of FY 17.	9/30/2017

CONTACT INFORMATION. If you have any questions regarding this response, please contact Carrie Hallum, OEI's Audit Follow Up Coordinator, at 202-566-1274.

cc: Carrie Hallum
Robert McKinney
Sean Kelly
Ken Schifter
Renee Gutshall
Karen Maher

Appendix D

UNITED STATES ENVIRONMENTAL PROTECTION AGENCY

WASHINGTON, D.C. 20460

OFFICE OF
ENVIRONMENTAL
INFORMATION

[June 19, 2017]

OEI's Updated High-Level Corrective Action Plan

High-Level Corrective Action Plan as of June 19, 2017:

OEI's RESPONSE TO REPORT RECOMMENDATIONS #3 AND #4:

Recommendation	Agency Response	Revised Recommendation	Agency Response	Planned Milestone Date
3.Implement a process to maintain a listing of agency contractor personnel who have significant information security responsibilities that require role based training, and validate that all relevant contractor personnel have completed the required role-based training.	We disagree to some extent. It is the responsibility of the COR to inform the ISO of the contractor personnel that require privilege access, that person also initiates the documentation for the person to have privilege access. The IMO also validates the documentation to ensure that the person has	Implement a process that requires appropriate Agency personnel to maintain a listing of contractor personnel who have significant information security responsibilities required to take role-based training. This process should require appropriate Agency personnel	OEI agrees with the revised recommendation, with a few clarifications. First, we would ask that the recommendation be changed from "Implement a process" to state that "OEI will work with the Assistant Administrator for Administration and Resources Management to implement a process." This may require actions from	12/31/2018

Recommendation	Agency Response	Revised Recommendation	Agency Response	Planned Milestone Date
	completed the training and signs the RoB. The ISO and System Owner have "Line of Sight" on their IT Personnel, it should not fall upon OEI to maintain a dynamic list of the Agency's contractors. However, OEI agrees that it should confirm (e.g., through communication from the CO, COR, IMO, or ISO—process to be determined) that all required training has been performed.	to validate and report to the Senior Agency Information Security Officer that all relevant contractor personnel have completed role-based training.	Contracting Officer Representatives and would necessitate coordination with OARM. Second, OEI would attest that Agency personnel should respond to the Chief Information Security Officer, not the SAISO, that all relevant contractor personnel have completed role-based training.	
4. Include the number of contractors who have significant information security responsibilities and have completed the required role-based training in the EPA's Federal Information Security Modernization Act reports submitted to the Office of Management and Budget	OEI agrees in part that based upon a recent change in A-130, Appendix I, this requirement can be met by the end of FY 17.			09/30/2017

Appendix E

Distribution

The Administrator
Chief of Staff
Assistant Administrator for Environmental Information and Chief Information Officer
Assistant Administrator for Administration and Resources Management
Agency Follow-Up Official (the CFO)
Agency Follow-Up Coordinator
General Counsel
Associate Administrator for Congressional and Intergovernmental Relations
Associate Administrator for Public Affairs
Principal Deputy Assistant Administrator and Deputy Chief Information Officer, Office of Environmental Information
Deputy Assistant Administrator, Office of Administration and Resources Management
Director, Office of Information Security and Privacy, Office of Environmental Information
Director, Office of Acquisition Management, Office of Administration and Resources Management
Director, Office of Resources, Operations and Management, Office of Administration and Resources Management
Deputy Director, Office of Resources, Operations and Management, Office of Administration and Resources Management
Audit Follow-Up Coordinator, Office of the Administrator
Audit Follow-Up Coordinator, Office of Environmental Information
Audit Follow-Up Coordinator, Office of Administration and Resources Management
Audit Follow-Up Coordinator, Office of Acquisition Management, Office of Administration and Resources Management