PORTSMOUTH / PADUCAH PROJECT OFFICE

Information Technology Strategic Plan

Aligning Secure Technologies to Accomplish Mission

Information Technology Strategic Plan

FY2019 - 2022

Revision Change Log

Revision	Section	Description	Date
0	All	Initial development	2/2019

Approvals for the PPPO IT Strategic Plan

Approval: Robert E. Edwards III 2/19/19
Robert E. Edwards, III – Manager — Date

Concurrence: 02/07/19
Joel B. Bradburne – Deputy Manager — Date

Concurrence: 1/29/19
James Woods – IT Specialist — Date

Concurrence: 1/29/19
Abraham Getchell – IT Specialist (INFOSEC) — Date

Concurrence: Jennifer Woodard 1/29/19
Jennifer Woodard – Paducah Site Lead — Date

Concurrence: 1/29/19
Jeff Bettinger – Portsmouth Site Lead — Date

Concurrence: 1/30/19
Reinhard Knerr – DUF6 Federal Project Director — Date

Concurrence: 29JAN19
Mark Allen – Security Team Lead — Date

Concurrence: 1/29/2019
Bart Simpson – IT Manager, EOTS Contractor — Date

Information Technology Strategic Plan Fiscal Years (FY) 2019 - 2022 "*One* PPPO"

1. Executive Summary

The mission of the Portsmouth/Paducah Project office (PPPO) is to conduct safe, secure, compliant, and cost effective environmental clean-up of the Portsmouth and Paducah Uranium Enrichment Sites on behalf of the local communities and the American taxpayer. The PPPO's Information Technology and Cyber Security capability plays an important role in fulfilling this mission as an essential support function.

The PPPO Information Technology (IT) Strategic Plan provides five elements that will align secure methodologies and technologies to support the Department of Energy (DOE) Office Of Environmental Management's (EM) mission of reducing risk and environmental liabilities by implementing technology to enhance the effective, safe and secure completion of the PPPO clean-up mission. The *One*PPPO initiative will provide a unification of the information systems to gain efficiencies and improve the security posture, with an integrated approach to the IT infrastructure to provide effective and consistent communications across all projects.

PPPO IT Strategic Elements *One*PPPO initiative will provide a unification of the information systems to gain efficiencies and improve the security posture	
Elements	**Benefits to PPPO**
Virtualized Infrastructure	✓ Reduced hardware costs ✓ Faster Provisioning and deployment ✓ Improves Disaster Recovery ✓ Reduction in energy costs ✓ Increased IT Staff Productivity
Zero Client Computing	✓ Reduces Computer Footprint for End User ✓ Easier Computer Sharing ✓ Faster Provisioning and Deployment ✓ Reduction in Energy Costs ✓ Added Security
PPPO Shared Services Portal	✓ Integration of internal and external data sources ✓ Centralized storage for collaboration (EEOICPA, EIC, Risk Management, Permitting, etc.,) ✓ Consistent Information and Processes ✓ Federated PPPO
Site Wide Wireless Networks	✓ Productivity Through Mobility ✓ Network Scalability ✓ Improved Responsiveness in Field ✓ RFID for cylinder and D&D waste tracking
Enterprise IT Procurements	✓ Economies of Scale ✓ Improved Procurement Process ✓ Standardized hardware and software ✓ Leverage IT skillsets and lessons learned

The foundation to support the PPPO elements are implementation of consistent electronic records management systems, enterprise mobility through development of mobile applications, standard hardware and operating systems, and robust mobile device management. These communications must provide a robust security program to protect and prevent any loss or compromise of data. Successful implementation of these initiatives will provide fast and reliable access to consistent information and the quick application of lessons learned, supporting clean-up of DOE EM's last two gaseous diffusion plants as well as conversion of the depleted uranium hexafluoride (DUF6) cylinders at the sites.

The collaboration within the EM organization and other sites is critical to the success of project execution and good stewardship of DOE assets to perform remediation, deactivation, and demolition of facilities. This will be accomplished through integrated project teams (IPT) within PPPO and targeted teams across the EM and DOE complex.

PPPO will continue to partner with the Environmental Management Consolidated Business Center (EMCBC) IT team to integrate business and procurement processes along with close interaction of IT planning goals and electronic records management policies. This relationship has been utilized to successfully achieve goals such as HSPD-12, remote access capabilities, consolidation of wireless telecommunication contracts and alignment of procedures and processes. Moving forward it can provide even more benefit to the implementation of the PPPO IT Strategic Plan and elements while supporting the project missions.

Implementing the elements outlined in this plan and working collaboratively, the PPPO can streamline the IT support process and provide a secure and strong infrastructure to allow the Federal and contractor teams to perform at an optimal level. This will support more efficient field activities and flexible work environments that remove limitations for users and allow for more rapid and cost effective deployment of personnel to the areas where the work is to be completed.

An effective cyber security capability, managing risk to within the organizational risk tolerance, allows PPPO leadership to have confidence the information they leverage during the decision-making process has been protected from unauthorized or accidental disclosure, intentional or unintentional modification, and will be available to them when needed. In addition, this capability protects DOE and PPPO's reputation, and aids senior officials in solidifying public trust; a necessary factor for mission accomplishment. This five-element Cyber Security Strategic Plan charts a course to designing, implementing, and sustaining an effective cyber security capability across federal and contractor PPPO organizations in support of mission accomplishment.

(5) Strategic Cyber Elements

- ✓ Establish a funding stream for cyber security operations and oversight
- ✓ Establish an enterprise risk management strategy
- ✓ Establish an enterprise cyber security architecture
- ✓ Establish an oversight system to measure program compliance and maturity
- ✓ Foster collaboration with government and industry partners

2. PPPO IT Strategic Elements

The PPPO IT Teams will continue the improvement and advancement in operations and performance through the review and implementation of new technologies such as: connectivity (site, internet, and Headquarters (HQ)), wireless networks, mobile devices, operating systems, hardware, software development, electronic records management, shared services, and remote access. The ability to deploy and support technology that can provide real time access to PPPO wide resources allows for users to more efficiently and effectively oversee work in the field. This additional oversight and integration into field activities will lead to safer and more collaborative operations with PPPO contractor organizations. The ability to work safer and more effectively will allow the reduced Federal staff and contractor teams accomplish the clean-up missions of the Portsmouth and Paducah sites safer and within the project schedules.

The PPPO IT team provides oversight and guidance to all PPPO site contractors to ensure collaboration and teamwork among all contractors in regards to IT work being done at the sites. This effort allows the PPPO as a whole to remain compatible and effective in completing work at all sites in regards to IT no matter the site. This oversight provides all contractors with the same guidance and interpretation of requirements to eliminate any duplication of IT effort. The PPPO IT team also provides guidance for the cyber security programs at all PPPO sites to improve the security footprint of the sites. The PPPO IT team assists with planning and review of contract transitions to provide guidance to incoming and outgoing contractors on DOE requirements and mission specific goals. This oversight allows PPPO and the contractors to apply lessons learned among PPPO operations. It also facilitates the sharing of lessons with the EM HQ to help in continued improvement of the EM IT program.

The following five strategic elements have been established to support the mission by enhancing the effectiveness of users and reducing the cost of large IT support teams:

Strategic Element #1 – Implementation of Virtualized IT Infrastructure

EM IT Strategic Plan – Strategic Goal 2 - Objective 2.3: Deploy enhanced or new innovative Green IT solutions to meet EM mission needs

Implementing a virtualized IT infrastructure reduces cost of hardware and maintenance support contracts by reducing the overall foot print of hardware. The reduced hardware allows for less heat generation and requires less cooling to maintain proper operating environments. This reduction in cooling and power requirements reduces the overall carbon footprint of the IT infrastructure by reducing greenhouse gases. This reduction in hardware and centralization of equipment can be managed by less IT personnel reducing the cost of management and support by reducing downtime for maintenance and reducing the deployment times of new applications and support systems.

Strategic Element #2 – Implementation of zero client computing

EM IT Strategic Plan – Strategic Goal 2 - Objective 2.3: Deploy enhanced or new innovative Green IT solutions to meet EM mission needs

Deployment of zero client endpoints to users removes bulky computer hardware from users work spaces and reduces the power and heat within those spaces, and provides longer device life. These zero clients reduce the deployment and support time for IT to manage user moves and personnel changes. The systems can be managed from central consoles allowing desk side support personnel to be more efficient. The non-persistent storage utilized by zero clients adds an in-depth cyber security approach to negative events by reducing the

time to clean up malicious software or exfiltration attempts.

Strategic Element #3 – PPPO Shared Services

EM IT Strategic Plan – Strategic Goal 2 - Objective 2.1: Enhance and promote collaboration capabilities that enable seamless teamwork across EM sites and partners

A shared services portal for the PPPO provides a centralized location for application and data collaboration for activities like regulatory permits, risk modelling, cyber risk tracking, EEOICPA, Environmental Information Center (EIC), and other activities that would have multiple users internal and external to PPPO come together on projects. This collaboration is a single point of communication and control for both public and sensitive documents that users can readily access to view and provide input or comments along with controlled locations for approved decision documents and other information regarding site projects.

The OnePPPO initiative is integral to intra-organization information sharing with the migration of information systems to the new pppo.gov namespace, establishment of the PPPO extranet (virtual private network_(VPN) mesh network), and modification of email filtering. This consolidation of services will work in real time to enhance the efficiency and quality of products. The Risk Tracking System is an example that already has been deployed in the shared services model and in use by all PPPO contractors and the data is used by both PPPO and EM HQ federal oversight for risk management and is key in the establishment of new systems and Continuous Monitoring of existing PPPO The Federal Information Security Management Act (FISMA) boundaries.

Strategic Element #4 – Site wide Wireless Networks

EM IT Strategic Plan – Strategic Goal 5 Objective 5.2: Ensure mission information is electronically available

Deployment of wireless infrastructures across all PPPO sites increases the productivity of users by allowing for users to be completely mobile while performing field oversight activities and still have access to all internal resources. This mobility, along with the ease of deployment of new field operations centers, reduces the cost of personnel relocation or increases by reducing the time for deployment and eliminating the need for IT infrastructure cabling. The wireless solutions are easily expandable with limited infrastructure needs to allow for rapid expansion of work tasks into new facilities or projects across the sites. When deployed across the PPPO, the wireless infrastructure will offer internal, shared site and guest access that can be utilized by all DOE employees and contractors, keeping them connected anywhere on the site their work requires.

Figure 1 The potential to improve data analytics with real time tracking of DUF6 cylinders is an example of integrating wireless and Radio-frequency identification (RFID) technologies to improve performance and reduce costs.

Strategic Element #5 – Enterprise IT Procurements

EM IT Strategic Plan – Strategic Goal 4 Objective 4.3: Achieve EM-wide IT Portfolio Management

An enterprise procurement approach will allow all of the PPPO IT Teams to take advantage of work performed in determining technology needs and requirements without having the resources or budget in place to do so internally. This approach will be beneficial to the PPPO in that IT, Cyber Security and other miscellaneous IT procurements can be budgeted at an enterprise level and take advantage of the economies of scale and reduce the overall purchase costs. This approach also will build in an enterprise architecture to standardize the PPPO IT Infrastructures by gathering requirements across all sites and building in a standardized baseline for hardware and software. By standardizing the hardware and software the PPPO IT Teams have the ability to work collaboratively on deployments and outages which in turn reduces outages and decreases cost for third party support effort.

2.1 Effective High performance IT workforce

EM IT Strategic Plan – Strategic Goal 3 Objective 3.2: Enhance the EM IT/IM workforce through professional development

The PPPO IT teams will continue to keep trained IT professionals on staff and continued education for IT professionals is a high priority and all PPPO sites will maintain robust training programs. A documented training plan will pay dividends to ensure that each site and project has a training plan in place to ensure that the right training is given to the right employees at the right time. These programs will allow IT professionals to achieve and maintain certifications and become skilled with the newest technologies. The PPPO IT program across all sites is also recruiting recently graduating professionals to utilize as interns as PPPO trains and prepares for work in the growing IT environments. All sites participate in hosting solution specific training is use by all PPPO IT teams to help keep staff skillsets current and leverage training dollars to allow for more staff to attend training at lower costs.

3. PPPO Cyber Security Integration

The day to day business of cyber security is IT-centric and PPPO's Information Technology organization will continue the integration of Cyber Security in the delivery of services. PPPO's IT team will continue to provide infrastructure to cyber security with initiatives such as: active scanning, wireless protection, working with the EM Mission Information Protection Program (MIPP) team, patch management, software quality assurance, configuration management, continued review of lifecycle plans for legacy applications and hardware, implementation of new cyber security technologies, EM driven cyber initiatives, attendance of DOE sponsored cyber security events, and industry training.

The PPPO Cyber Security Strategic Plan consists of five strategic elements, associated enabling objectives, and risks to successful implementation. The implementation of these elements ensure

cyber security-related risk is being managed to within the organizational risk tolerance and the PPPO's cyber security capability is aligned with the mission at all sites.

Strategic Element #1: Establish a funding stream for cyber security operations and oversight

EM Strategic Plan – Strategic Goal 1 Objective 1.4: Establish total cost ownership and lifecycle management and cost for cyber security solutions

To effectively support the implementation and governance of a mission focused cyber strategy an established funding stream is required. This funding stream will provide a structure to enable timely decisions for short and long term staffing and procurements.

Strategies:

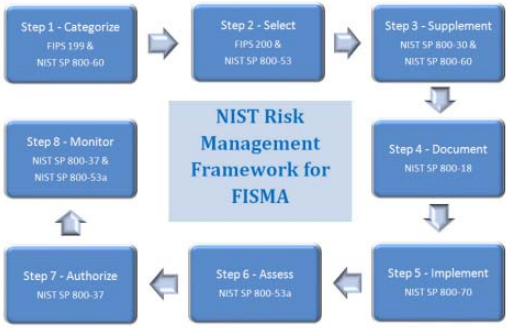
- ✓ Establish funding baseline for cyber security operations and oversight
- ✓ Develop five year cost projections for cyber security operations and oversight
- ✓ Coordinate with finance and provide appropriate justification for funding

Strategic Element #2: Establish an enterprise risk management strategy

EM Strategic Plan – Strategic Goal 1 Objective 1.3: Improve data quality of EM cyber related information for reporting, compliance, and use

A risk management strategy is at the core of an effective cyber security program. A structured approach establishes a repeatable process through which cyber security-related risk is framed, assessed, responded to, and monitored on an ongoing basis at the organization, mission-related process, and information system tiers. A comprehensive framework involving technical cyber security personnel, management, and leadership from within contractor organizations and the federal office ensures risk-based decisions are visible at all levels of the organization and take into consideration all applicable information. Leveraging automation to execute the framework where efficiencies can be gained ensures processes are executed consistently, resulting in output that remains viable across contract transitions, federal oversight personnel changes, and leadership evolutions.

Central to this approach is the identification of information system assets. This identification process includes developing and maintaining an inventory of classified and unclassified general support systems, major applications, industrial controls systems, and national security systems (Objective 2.1). Executing the information system authorization process and applying minimum security control baselines to all inventoried organizational information systems ensures risk is maintained at an acceptable level (Objective 2.2). Maintaining compliance with regulatory requirements having implemented basic cyber security capabilities is considered the minimum performance standard. Once compliance has been obtained and consistently maintained, the maturation to a risk-based, intelligence-driven approach is a natural evolution, resulting in the fielding of advanced capabilities focused on countering specific threats targeting PPPO, DOE,



or the US government as a whole. (Objective 2.3). Finally, it is essential to ensure this strategy is documented in a Risk Management Approach Implementation Plan (RMAIP) and receives leadership buy-in and sign-off (Objective 2.4).

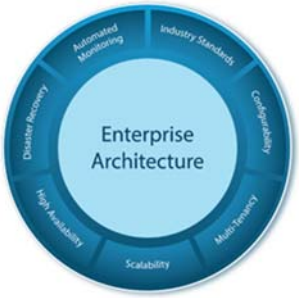
Strategies:

- ✓ Develop and maintain an information system inventory.
- ✓ Obtain and maintain compliance with regulatory requirements.
- ✓ Establish and mature a risk-based, intelligence-driven doctrine.
- ✓ Develop a PPPO Risk Management Approach Implementation Plan.

Strategic Element #3: Establish an enterprise cyber security architecture

EM Strategic Plan – Strategic Goal 1 Objective 1.2: Enhance situational awareness of cyber security threats and vulnerabilities to EM mission systems and information

The establishment of an enterprise security architecture is essential in ensuring consistent and effective implementation of technology and processes across disparate PPPO organizations and information systems. Central to this approach is working with federal and contractor Information Technology personnel to establish a common information technology and security architecture within organizational information systems (Objective 3.1). To maintain this consistency across the PPPO complex, it is imperative that software and hardware costs associated with cyber security are reimbursed on fixed-price contracts in Portsmouth and Paducah (Objective 3.2). In addition, as has been seen with recent adoption of cloud services within the Department of Energy (DOE) and across the government as a whole, significant efficiencies are realized when a shared services architecture is leveraged. Where applicable, a shared services architecture designed, implemented, and managed at the PPPO federal office should be leveraged (Objective 3.3). For low-risk uses such as public websites, a cloud computing strategy should be developed to ensure consistent and approved use of this technology across PPPO organizations (Objective 3.4). Finally, to ensure consistent implementation of security control across organizational information systems, as well as so security controls are selected for implementation which address the risks unique to PPPO organizations and systems, a security control overlay should be developed, approved, and integrated into organizational System Security Plans (Objective 3.5).



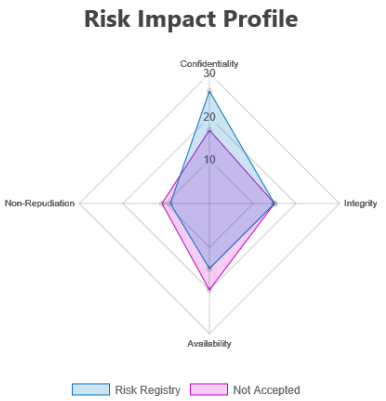
Strategies:

- ✓ Establish a common technology platform across disparate contractor organizations.
- ✓ Reduce heterogeneous architecture by reimbursing hardware and software costs.
- ✓ Establish centralized shared services where efficiencies can be gained.
- ✓ Establish and document an approach to leveraging government-vetted cloud services.
- ✓ Develop overlays for information systems to mitigate unique risks.

Strategic Element #4: Establish an oversight system to measure program compliance and maturity

EM Strategic Plan – Strategic Goal 1 Objective 1.2: Enhance situational awareness of cyber security threats and vulnerabilities to EM mission systems and information

Establishing a formalized cyber security oversight approach serves several purposes for PPPO: Ensures continuous monitoring is being executed per regulatory requirements, provides validation that contract scope is being executed effectively by contractors at the sites, and serves as an assurance system providing a level of confidence to leadership that the security and integrity of information being used in the decision-making process has been maintained. The fundamental component of this oversight system is the establishment of a Cyber Security Working Group and the delegation of the Risk Executive Function to this group (Objectives 4.1 and 4.2). Ensuring critical cyber security deliverables are integrated into all time and materials and fixed price contracts within PPPO, alongside of meaningful metrics in Quality Assurance Surveillance Plans (QASP), is essential in ensuring federal oversight staff has the information they need to conduct oversight activities (Objectives 4.3 and 4.4). A large part of ensuring cyber security capabilities are effectively supporting the mission as needed is to ensure that compliance is not just being met, but also are functioning effectively on an ongoing basis. As such, a capability maturity model should be established and both programmatic and technical assessments should be conducted measuring cyber security capabilities against this model (Objectives 4.5, 4.6, and 4.7). Finally, the integration of cyber security oversight with the Safeguards and Security and Quality Assurance teams ensures security matters are addressed as a single issue and surveillances and assessments are executed per organizational procedures and consistently over time (Objective 4.8).



Strategies:

- ✓ Establish a Cyber Security Working Group.
- ✓ Integrate critical cyber security deliverables into contracts.
- ✓ Establish meaningful cyber security metrics.
- ✓ Establish a cyber security capability maturity model focusing.
- ✓ Conduct programmatic assessments of contractor cyber security programs.
- ✓ Conduct technical testing of contractor-operated information systems.
- ✓ Integrate and coordinate oversight activities with QA and S&S.

Strategic Element #5: Foster collaboration with government and industry partners

EM Strategic Plan – Strategic Goal 1 Objective 1.1: Expand cyber security collaboration across the EM enterprise

PPPO will implement an assortment of approaches to promote collaboration throughout PPPO, EM, DOE, and industry. The creation of working groups will allow the organization to collectively leverage knowledge and solutions, and mature the posture of cyber security.

Strategies:

- ✓ Collaborate with other DOE sites and HQ to develop solutions to unique problems.
- ✓ Establish relationships with other government agencies to learn what works in government at large.
- ✓ Strengthen ties with Intelligence Community partners for the purpose of intel sharing.

4. Complex Wide Collaboration

The PPPO IT team will continue to work closely with other EM sites to gather lessons learned and IT strategies utilized to achieve many goals. This effort is already in place with the EMCBC and EM HQ MIPP team and has proven to be of great benefit to PPPO and other sites. Currently the PPPO IT team works closely with the EMCBC, EM HQ, East Tennessee Technology Park and Waste Isolation Pilot Plant. PPPO is planning to work with other sites to take advantage of their larger IT teams and more abundant resources for learning opportunities and to resolve PPPO issues. The PPPO IT team has been the first to deploy several cyber security tools and products and continues to provide results and findings to all EM sites to assist in their deployment of these products. EM HQ is undertaking the task to prepare and deploy a centralized enterprise architecture and strategic planning approach to IT across the EM complex. This planning approach will allow the small and large sites take advantage of work performed in determining technology needs and requirements without having the resources or budget in place to do so internally. This approach will be beneficial to PPPO in that IT, Cyber Security and other miscellaneous IT procurements can be budgeted at an enterprise level and purchased at the same level to be rolled out to the sites with lower site IT and Cyber Security costs. Additionally t the PPPO IT Team will also form a control board that will help to keep configurations consistent and appropriate to all EM sites instead of sites selecting tools, hardware, applications or systems specialized to one site. Appendix A contains a crosswalk of the EM IT Strategic Goals with a current status of the PPPO IT Strategic Goals. The PPPO plan is based on PPPO mission tasks and does match up with the majority of the EM goals. The flexibility to follow EM enterprise guidance has allowed PPPO to still achieve site specific tasks.

The relationship between PPPO and EMCBC has greater significance and a higher level of collaboration in that the EMCBC provides many business support functions. The relationship is critical in ensuring the PPPO IT mission is successful on all fronts. The collaboration efforts currently underway include synchronization of enterprise approaches, alternate processing site facilities, remote Source Evaluation Board (SEB) activities, cross site integrated lessons learned, training opportunities, integrated project planning and management level budget and planning involvement. Future activities will be anchored around the shared services needs for both sites and EM, platform and system standardization, management approach and cyber security integration. With the EMCBC and PPPO IT teams working together it creates a unique structure that can leverage many individual skillsets and utilize enterprise planning and project approaches to significantly increase the successfulness of IT projects across both sites.

5. PPPO IT and Cyber Security Working Groups

A key element of establishing "*One*-PPPO" is the formation of the PPPO IT and Cyber Security Working Groups with members from DOE and each of the contractor teams. The working groups are critical to the successful implementation of the PPPO IT Strategy and Plan, by bringing together the stakeholders to define, design, implement, and operate the strategic projects. The objective of the working groups are to implement the IT strategic goals one through five by assisting to determine the hardware, software and processes used across all PPPO sites to support the PPPO clean-up mission safely and securely utilizing the ever changing technology that becomes available.

To ensure effective communication the working groups will establish a charter and meet on a regular monthly basis discuss ongoing projects, future planning, site needs, data calls and other IT and Cyber Security activities related to this plan. Additionally, the working groups will meet annually at one of the PPPO sites to maintain open communications and support the integrated approach to IT and Cyber Security within the PPPO.

The PPPO Shared Services Portal will provide the platform for federated collaboration across for review and tracking performance of these projects. To ensure that Cyber Security is integrated into IT projects, the IT working group shall include members from the PPPO cyber security organizations.

6. Summary

The PPPO team has planned the strategies for the PPPO sites to be in alignment with the overarching DOE EM Strategies. The synergies of this planning will enable PPPO to meet the needs of their user communities while meeting the mission needs of EM and the Department of Energy.

Appendix A is a list of outside drivers that guide the direction of the IT and Cyber Security programs across PPPO. PPPO will establish a risk based approach to project management lifecycles, by continual review of new technology and advancements across the EM complex, the PPPO IT team can provide a more secure, efficient and effective infrastructure for the PPPO team to utilize to achieve the mission goals. Appendix B contains the list of PPPO IT Hardware and Software that apply to the key operations across the PPPO IT Infrastructures. Appendix C outlines the list of PPPO Cyber Security Hardware and Software for all PPPO FISMA Boundaries.

APPENDIX A: Outside Drivers

Driver	Impact
EM Mission Focus Areas	EM's strategic focus areas of safety, project management, and accelerated site closure represent key elements that affect EM IT priorities including the need for increased program-wide IT collaboration, risk-informed decision-making, shared services, and the need for more robust governance of IT investments that support mission needs.
Programmatic Budget Pressures	Operating in a constrained budget environment demands a focus on eliminating redundancies, prioritizing existing service delivery requirements, and only investing in IT solutions that are cost-effective and demonstrate value.
EM, OICO, OMB Data calls	With the ever increasing flow down of data calls from many levels, the IT organizations must be prepared to respond timely and accurately, this will be a challenge for many organizations operating in a Firm Fixed Price (FFP) contract vehicle due the increased number of these requests.
Retiring Workforce	Requires the development and execution of strategies to attract and retain a pipeline of talent that can support EM's current and future IT mission needs, and to establish a knowledge management capability available for the current and future EM workforce.

Federal IT Mandates and Legislative Requirements	**The following government-wide directives provide access to existing government information assets that EM can benefit from:** • Federal Information Security Management Act (FISMA) of 2002 • National Institutes of Standards and Technology (NIST) Standards and Guidelines • Federal Information Technology Acquisition Reform Act (FITARA) (December 2014) **Office of Management and Budget (OMB) Policies and Directives, such as:** • OMB Circular No. A-130 Management of Federal Information Resources (November 28, 2000) • M-10-06 Open Government Directive (December 8, 2009) • 25 Point Implementation Plan To Reform Federal Information Technology Management (December 9, 2010) • Federal Cloud Computing Strategy (February 8, 2011) • Federal Information Technology Shared Services Strategy (May 2, 2012) • The Common Approach to Federal Enterprise Architecture (May 2, 2012) • Digital Government: Building A 21st Century Platform To Better Serve The American People (May 23, 2012) • M-12-18 Managing Government Records Directive (August 24, 2012) • Executive Order 13636 Improving Critical Infrastructure Cybersecurity (February 12, 2013) • M-13-09 Fiscal Year 2013 PortfolioStat Guidance: Strengthening Federal IT Portfolio Management (March 27, 2013) • M-13-13 Open Data Policy – Managing Information as an Asset (May 9, 2013) • OMB Circular No. A-11 Part 6, Section 220 Cross-Agency Priority (CAP) Goals and Federal Performance Plan (July 26, 2013) • M-14-08 Fiscal Year 2014 PortfolioStat (May 7, 2014) • Executive Order 13693 Planning for Federal Sustainability in the Next Decade (March 19, 2015)

Departmental Orders	**DOE Orders such as:** • 203.2 Mobile Technology Management • 205.1B Chg 3 Department of Energy Cyber Security Program • 243.1B Admin Chg 1 Records Management Program • 206.1 DOE Privacy Program • 415.1 Chg 2 Information Technology Project Management
Programmatic Requirements	**Such as:** • Risk Management Approach Implementation Plan (RMAIP) Standard Operating Policies and Procedures (SOPP)
Frequency and Sophistication of Cybersecurity Threats	Requires increased situational awareness and vigilance in enhancing our ability to identify, protect, detect, respond, and recover from cyber-related events.

APPENDIX B: PPPO IT Hardware and Software List

Hardware	Application
Cisco ASA's	Utilized to provide firewall and network segmentation across boundaries including interconnected VPN mesh networks and shared operations.
Cisco Routers	Utilized for intersite and internet based routing operations.
Cisco Switches	Utilized for distribution and campus wide infrastructure.
Cisco Wireless	Utilized for end user wireless connections and guest access to network resources.
Software	**Application**
Microsoft Windows	Standard desktop operating system for end user access to network resources.
Microsoft Office	Standard application for day to day word processing, spreadsheet and general office activities.
Microsoft SQL	Standard database server for applications and services.
Microsoft SCCM Server	Standard server for providing system imaging, patching, compliance and other desktop support functions.
Microsoft Server	Standard server operating system for providing system services.
Microsoft Exchange	Standard system for e-mail across the sites.
Microsoft SharePoint	Standard web server for intranet, shared services and site wide applications.
Skype for Business	Standard web collaboration, instant messaging and communication server.
Adobe PDF	Standard format and application for PDF document reading, review and creation.

VMware	Standard virtual server environment for providing IT services and VDI across the sites.
Blackberry UEM	Standard MDM server for providing mobile device services.
GimmalSoft	Standard application for the Electronic Records Management Systems.
Entrust	Standard e-mail encryption software agent.
Sherpa E-Discovery	Standard application for FOIA and Litigation discoveries.
Redhat Linux	Standard server operating system required for applications requiring a unix / linux backend.

APPENDIX C: PPPO Cyber Security Hardware and Software List

Category	Vendor	Product
Operational		
Email Scrubbing	Cisco	Email Security Appliance (w/ Security Management Appliance)
Web Scrubbing	Cisco	Web Security Appliance (w/ Security Management Appliance)
Network Firewall	Cisco	Adaptive Security Appliance, FirePOWER
Network Access Control	Cisco	Identity Services Engine
Wireless Intrusion Detection/Prevention	Cisco	Mobility Services Engine
Network Intrusion Detection/Prevention	Cisco	Advanced Malware Protection
Active Directory Intrusion Detection/Prevention	Microsoft	Advanced Threat Analytics
Host Intrusion Detection/Prevention	Sophos	Endpoint Protection
Antivirus for Physical Endpoints	Sophos	Endpoint Protection
Antivirus for Virtual Endpoints	Sophos	Endpoint Protection
Device Control	Sophos	Endpoint Protection
Data Loss Prevention	Forcepoint	Data Loss Prevention Network
Vulnerability Scanning	Rapid7	Nexpose
Information and Event Management	Splunk	Splunk Enterprise
Full Packet Capture	Symantec	Security Analytics and Incident Response
Password Management	Thycotic	Secret Server On-Premise
Malware Analysis	ThreatTrack	ThreatAnalyzer
Honeypot	Thinkst	Canary
Network Monitoring	Ixia	CloudLens
Assessment		
Penetration Testing	Rapid7	Metasploit Pro
Vulnerability Scanning	Rapid7	Nexpose
Web Application Scanning	Acunetix	On Premise Pro
Web Application Scanning	PortSwigger	Burp Suite Professional