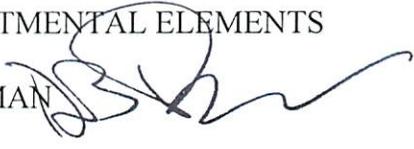




The Deputy Secretary of Energy
Washington, DC 20585

September 27, 2012

MEMORANDUM FOR HEADS OF DEPARTMENTAL ELEMENTS

FROM: DANIEL B. PONEMAN 
SUBJECT: Information Technology Modernization Strategy

Over the past several months the Administration has emphasized the need to improve government efficiency and reduce the cost of government services. The ongoing *Campaign to Cut Government Waste* is only one of the many recent government-wide efforts focused on these goals. To support these efforts at the Department of Energy (DOE) we are taking a comprehensive look at our commodity service areas to identify ways to improve efficiency and cut costs.

The DOE Chief Information Officer (CIO) and the National Nuclear Security Administration (NNSA) CIO were jointly tasked with developing a strategy to modernize our information technology (IT) environment and identify opportunities to share services, reduce costs, and leverage new technologies. They developed the attached IT Modernization Strategy to meet the overarching Administration goals while continuing to support DOE programs and missions. A strategic change of this scope does not happen overnight and we will be implementing elements of the strategy in phases.

The IT Modernization Strategy has been approved by DOE senior management and is attached as guidance for Departmental IT activity and decision-making. Please ensure this guidance is communicated to all those in your organization with IT acquisition and management responsibilities. The DOE OCIO and the NNSA OCIO will lead the implementation of the IT Modernization Strategy and will work with your organizations to ensure the expected outcomes are achieved.

Attachment



White Paper: DOE/NNSA Information Technology Modernization Strategy

INTRODUCTION

This white paper frames a Department of Energy (DOE) and National Nuclear Security Administration (NNSA) strategy for modernizing our Federal information technology (IT) as one of the foundations for management and operational excellence. It outlines some of the current challenges and key strategy points for modernization, along with existing efforts and their role in the strategy.

The DOE Strategic Plan establishes IT and cybersecurity as foundational to the achievement of the Department's mission while managing risks aggressively and effectively. This means building systems and infrastructure that are cost effective and support efficient operations, and ensuring the cutting edge application of technology and creative solutions in a framework that provides flexibility. Cybersecurity must be managed in the broader context of risk, with tailored protections and a continually evolving and responsive program that adjusts to changing threats, vulnerabilities, and needs. We will implement a Department-wide approach to risk management for unclassified and classified IT environments.

The DOE/NNSA IT Modernization Strategy (to include cybersecurity strategy) must be integrated with the overall DOE strategy from mission planning through performance and achievement of outcomes. The IT strategy takes into account the various business and mission strategies across the Department and is designed to enhance and enable those strategies; and the IT strategy addresses people issues, including the organizational alignment of personnel performing IT and cybersecurity processes, governance, and management.

Transforming the DOE and NNSA disparate IT systems into a modern, flexible architecture that maximizes the use of limited resources will be a multi-year effort requiring close coordination and unity of effort across the Department's Program and Functional Offices. This transformation also requires new levels of transparency into IT activities and costs so that corporate decision-making processes will lead to informed choices that enable the workforce of the future. The return on investment must be calculated in terms of mission effectiveness improvement, fiscal efficiency, and the enterprise risks associated with the project.

While this paper focuses on modernizing the unclassified Federal IT ecosystem, the principles herein are relatable to classified systems and the interface with DOE/NNSA site contractors. The DOE Chief Information Officer's (CIO) overarching strategic goals serve to guide this transformation:

- **Strategic Goal 1: Leverage Existing IT** - Leverage existing information technology and expertise to maximize mission accomplishment and reduce costs.
- **Strategic Goal 2: Foster New and Emerging IT** - Identify and foster new and emerging information technology to maximize mission accomplishment and reduce costs.

- **Strategic Goal 3: Strengthen IT Governance, Policy, and Oversight Processes** - Provide Departmental IT governance, policy, and oversight processes to ensure secure, efficient, and cost-effective use of IT resources.
- **Strategic Goal 4: Institutionalize Risk-Based Cybersecurity** - Strengthen enterprise situational awareness to foster near-real-time risk management and combat the advanced persistent threat; forge interagency and sector partnerships to protect critical infrastructure, promote information sharing, and advance technologies for cyber defenses.

THE CHALLENGE

Many Program Offices, Operations and Site Offices, and Functional Offices procure and manage separate IT services for DOE's approximately 15,000 Federal staff and a significant number of direct support service contractors. While this model enables the Department to customize IT infrastructure, systems, and services to meet its mission, it creates duplication of hardware, software, personnel, etc. It also fails to fully leverage available funding that could be utilized for direct mission activities. This model has led to commodity computing solutions that are both expensive and not in-line with modern computing trends. In addition, this model results in services that are fractured between programmatic lines further increasing costs, creating redundant investments, and limiting transparency.

As a result, DOE/NNSA's commodity IT environment currently includes numerous IT Directors; hundreds of IT operations personnel; more than 20 email systems; 46 datacenters of varying size; and over \$170 million in annual spending (although the actual spending is likely higher). While the customer base for each service varies, there is significant duplication, with over 120 separate instances of 26 commodity services.

Existing DOE/NNSA networks and services are only as interconnected within the agency as they are interconnected with other agencies or partners via the Internet. This level of interconnection is not optimal and limits the collaboration and coordination of people, knowledge and information necessary to fulfill DOE/NNSA's urgent and vital missions in science, energy and nuclear security. The lack of a more sophisticated and effective interconnection approach hampers the establishment and leveraging of common network and desktop configurations, creating inconsistency in our management of risk across similar environments.

The current decentralized approach to IT services acquisition leads to a significant number of contracts across the DOE/NNSA environment. Changing the nature of how DOE/NNSA procures Federal IT services could improve interconnectivity and performance and result in cost savings.

Additionally, there is currently limited insight into the details and metrics associated with activities, costs, and utilization in the DOE/NNSA environment. These types of metrics are what world-class businesses rely upon to manage their IT enterprise. Without this information, the full cost and the actual performance of DOE/NNSA's Federal commodity IT infrastructure and operations is uncertain and costs are likely greater than the above estimates.

DOE/NNSA's IT business model is unsustainable in an era of shrinking budgets and a government-wide shift towards a leaner government that leverages private sector capabilities and shared services (see [Digital Government: Building a 21ST Century Platform to Better Serve the American People](#)). Recent benchmarking by Gartner, Inc. shows that the IT infrastructure and service management cost difference between high performing IT organizations and less efficient IT organizations is an operational cost reduction of 41%. If DOE/NNSA IT organizations make a minor shift toward improving IT infrastructure and service management efficiency, a potential reduction of 20% in reported costs would result in nearly \$35 million a year being made available for higher DOE/NNSA priorities.

Individually, Program and Functional Offices are modernizing and improving the effectiveness and efficiency of their own IT operations. However, these independent activities will not lead to an enhanced IT management and operational environment for DOE/NNSA. Later in this white paper, those ongoing efforts and how they can support the modernization strategy will be discussed.

On the National Laboratory and Management and Operations (M&O) contractor landscape, IT services are generally more modern, sophisticated, and integrated. Each laboratory is chartered to look at its specific mission lines and build effective and efficient IT programs to service that scope of work. With differing missions at the M&O sites, the overall computing environment across laboratories, plants and other sites varies in terms of vendor diversity, architectures, and cyber security posture. From a micro perspective, DOE/NNSA has highly evolved point solutions or mini-architectures to service specific mission lines. However, from a macro perspective, there may be opportunities to use aggregate licensing to achieve volume discounts and integrate disparate but related data sources. Such efforts must be compatible with the missions and management structures of the M&Os.

THE IT MODERNIZATION STRATEGY

Future Office of the DOE Chief Information Officer

Today, the Office of the DOE CIO (OCIO) provisions voice, video, data, and application hosting and housing services to the Department's Federal employees and its direct support contractors. The DOE OCIO also provides desktop and worker productivity solutions, including mobile devices and cellular voice/data service. Additionally, the OCIO provides acquisition and enterprise license support for customers requiring hardware, software and support services.

Consistent with the ten strategic objectives in this IT modernization strategy, the OCIO will lead the alignment of structure, process and people to transition the vast majority of commodity IT services to an environment where the CIO serves as the Department's IT broker-advisor. The CIO will establish embedded customer relationship managers who understand and are committed to, and accountable for, meeting mission support requirements. This model will enable the CIO to focus on policy, governance, architecture and standards and the provisioning of core infrastructure and commodity IT through managed services, leveraging commercial

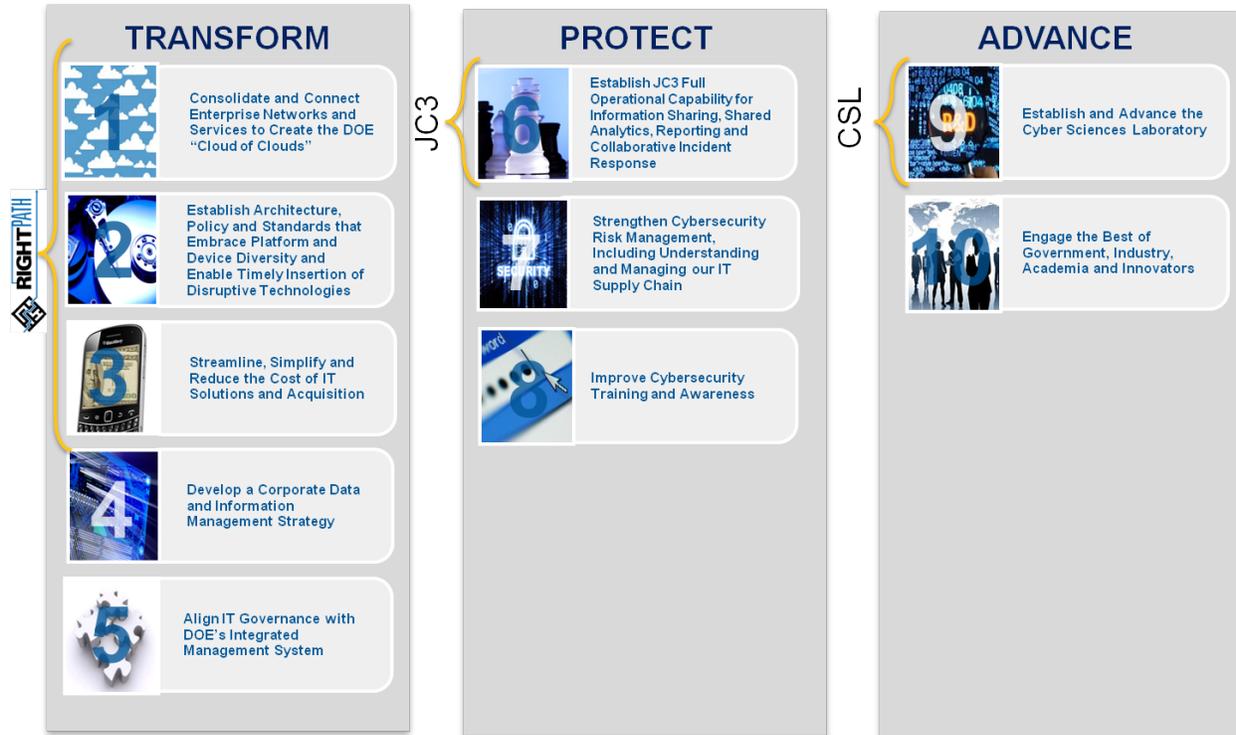
providers where possible, to meet mission outcome and security requirements. The broker-advisor model creates a modular IT system that enables structured flexibility to meet mission support requirements, while managing the complexity of the present and future environment to ensure effective interoperability and security while delivering efficient and reliable services.

The CIO believes that the “RightPath” framework (described later in this document) will demonstrate the effectiveness, efficiency and security of brokered services. Once determined to be scalable, the CIO proposes to roll services across the DOE/NNSA Federal IT ecosystem in partnership and collaboration with the Program and Staff Offices. As that effort progresses, the OCIO will move to place infrastructure as a service (IaaS), cloud IT service management and other contracts with commercial providers that can meet DOE/NNSA commodity IT level of service and security requirements so that legacy applications and services can be migrated to modern architectures, and where possible, legacy services can be transitioned and shut down.

Ten Strategic Objectives for IT Modernization

IT modernization will improve mission effectiveness, create fiscal efficiencies and provide the right level of security to our systems and information. The modernization strategy will take advantage of ongoing efforts and is integrated across three strategic pillars – Transform, Protect and Advance. The strategy leverages existing IT governance processes managed through the Information Management Governance Council (IMGCC), the Information Technology Council (ITC) and supporting working groups and integrated project teams (IPTs). This strategy will ultimately enable a fundamental shift in the amount of physical infrastructure needed to support employees and mission support operations, will remove geographic barriers to collaboration, and create a model environment within government that positions DOE as the employer of choice while improving job retention.

Individual objectives to meet the goals within each strategic pillar will be finalized and expanded in a follow-on implementation plan. The implementation plan will require a unified effort across the Department to develop the cost, risks and return on investments necessary for financial planning. A reasonable estimate is that about 10% of the planned FY 2013-2015 commodity IT spending should be re-allocated from low value to transformational investments (~\$15-18 million/year). The implementation plan will also establish the measures of performance and the operational metrics for management and oversight of sustained effectiveness and efficiency. The ten strategic objectives (10-Point Plan) for IT modernization at DOE are as follows:



Transform –Leverage existing and new activities to enable new technologies to be inserted into the overall architecture in a lean and agile manner to improve effectiveness and fiscal efficiency.

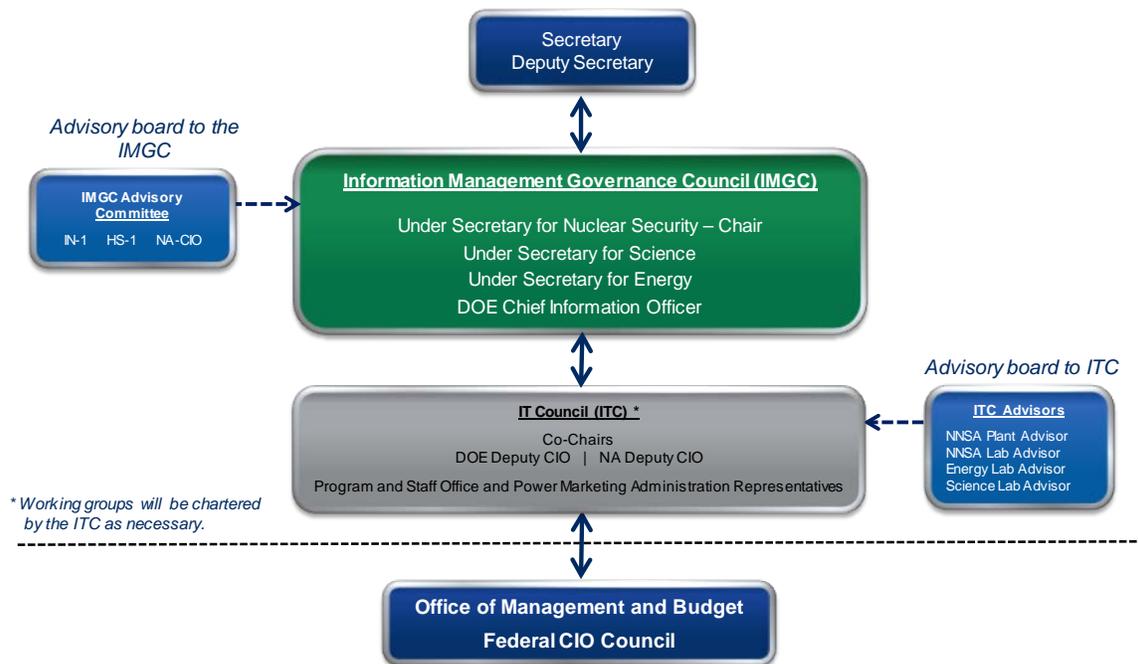
1. Consolidate and Connect Networks and Services to Create the DOE "Cloud of Clouds"

The most fundamental and critical objective of the strategy, the DOE "Cloud of Clouds", significantly reduces the number of redundant infrastructures and services (i.e., data centers, email systems, collaboration tools, etc.) to create an optimum suite of services that leverages commercial providers, where appropriate, to meet mission support requirements. This objective improves operational effectiveness, interoperability and security, while reducing cost and use of limited physical space. Furthermore, it reduces the number of systems and services that require direct management, reduces licensing and service fees, and reduces the number of Federal personnel and support contractors necessary to deliver effective IT services. Delivering on this objective also creates the technical strategy for achieving mission outcome.

2. Align IT Management and Governance

This second objective addresses structure, process and people to improve management and decision-making effectiveness by aligning IT personnel and resources to optimize their use. It also aligns IT governance structures and processes and creates stronger alignment of IT and cybersecurity decision-making to mission outcome through

improved vertical alignment and horizontal integration of IT governance with program and functional offices.



3. Establish Architecture, Policy and Standards that Embrace Platform and Device Diversity and Enable Timely Insertion of Disruptive Technologies

This third objective establishes the DOE CIO as a broker-advisor who will coordinate the architecture, policy, and standards necessary to enable mission outcomes. This objective addresses process improvements to reduce IT system complexity, improve security, and reduce the cost of entry for new technologies necessary to meet program and functional office requirements.

4. Streamline, Simplify and Reduce the Cost of IT Solutions and Acquisition

This fourth objective seeks to reduce the number of product and service procurement vehicles and to leverage the collective buying power of DOE to simplify and reduce the cost and complexity of acquisitions. The achievement of this objective will reduce acquisition workload. DOE/NNSA site contractors (including M&Os) will be engaged to achieve further enhancements, where appropriate. This objective also creates streamlined processes for matching requirements to alternatives for meeting those requirements and provides rapid provisioning of the selected solution. This improves efficiency and enables IT to be more agile in meeting mission support requirements. The objective will also identify changes in personnel alignment and skill sets necessary for

the effective relationship between procurement and IT personnel to deliver on the broker-advisor model.

5. Develop a Corporate Data and Information Management Strategy

This fifth objective creates a data and information lifecycle plan that ensures the right information is available at the right time. This objective improves mission effectiveness by enabling data driven decision-making. It also drives strategies that make data available for use in new ways for business intelligence and the delivery of citizen services, who may find new ways to leverage DOE/NNSA data. Implementation of the objective will also leverage governance improvements to create defined processes for aligning data creation and lifecycle management to support Departmental business and mission processes, including making that data discoverable, retrievable, reliable, and recordable in a format that supports use in both internal, and where needed, citizen-facing systems.

Protect – Leverage the Joint Cybersecurity Coordination Center (JC3) to improve information sharing, provide better operational awareness of security for corporate infrastructure, respond to incidents, and pro-actively build cybersecurity into new technology investments to ensure new technologies are appropriately secured throughout their lifecycle from design to retirement.

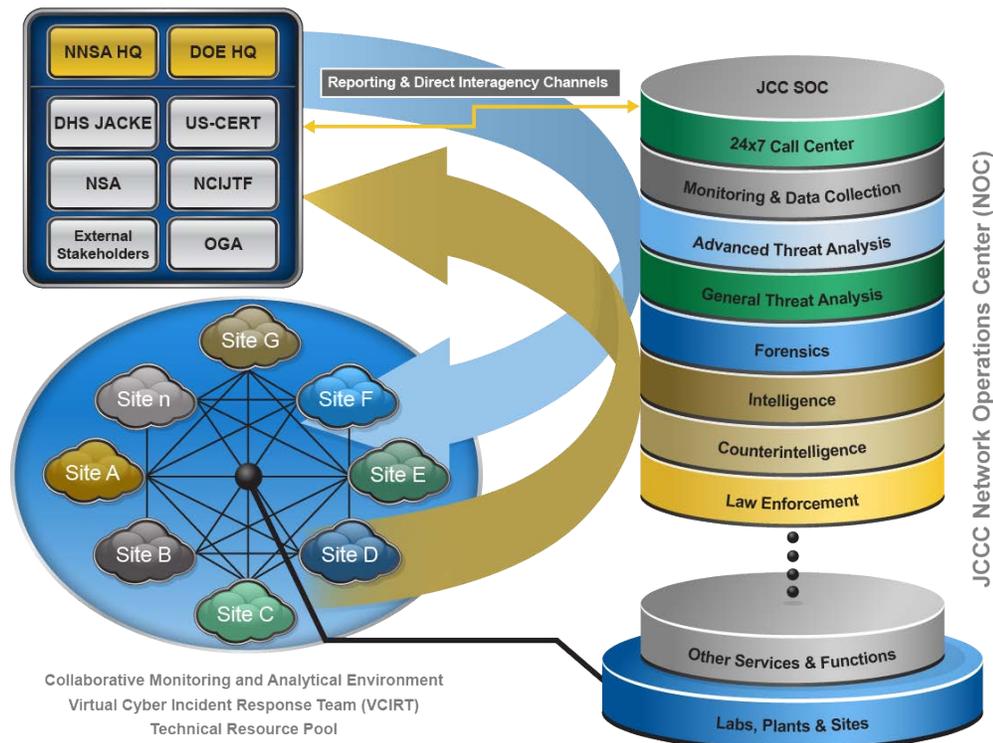
6. Strengthen Cybersecurity Risk Management, Including Understanding and Managing our IT Supply Chain

This sixth objective establishes structures, processes and people to continuously improve DOE/NNSA's management of cybersecurity risk, including the risk imposed by non-trusted supply chains. It establishes the corporate cybersecurity functions as well as the optional services necessary to meet the wide differences in security risk management requirements. This objective links to the "cloud of cloud" models and future standards to reduce complexity as an enabler to effective and efficiency cybersecurity and the management of the business and mission risks associated with it.

7. Establish JC3 Full Operational Capability for Information Sharing, Shared Analytics, Reporting and Collaborative Incident Response

This seventh objective leverages the collective, collaborative power of DOE/NNSA Federal and M&O contractor expertise to provide exceptional site and enterprise cyber situational awareness and effective cyber incident response; an incident response surge capability; timely and effective routine and urgent communication channels that enhance information sharing; a continuous learning cyber system in both the classified and unclassified environments; and integration of DOE/NNSA stakeholders to form a team approach to operational cybersecurity. It addresses critical improvements in cybersecurity operational strategies and the alignment of people and processes into a

new ecosystem that requires trust, collaboration, and coordination among all cybersecurity personnel to maximize the effectiveness of our security environment. This objective also reduces cost while improving cybersecurity readiness and response and support DOE (OE) Infrastructure Security and Energy Restoration capabilities for energy sector security.



8. Improve Cybersecurity Training and Awareness

This eighth objective addresses the weakest link in the cybersecurity value chain by delivering a rich training and awareness program that is tailored to the roles and responsibilities of each individual. It improves overall cybersecurity awareness and has the potential to reduce cybersecurity incident response costs by reducing the number and seriousness of avoidable incidents.

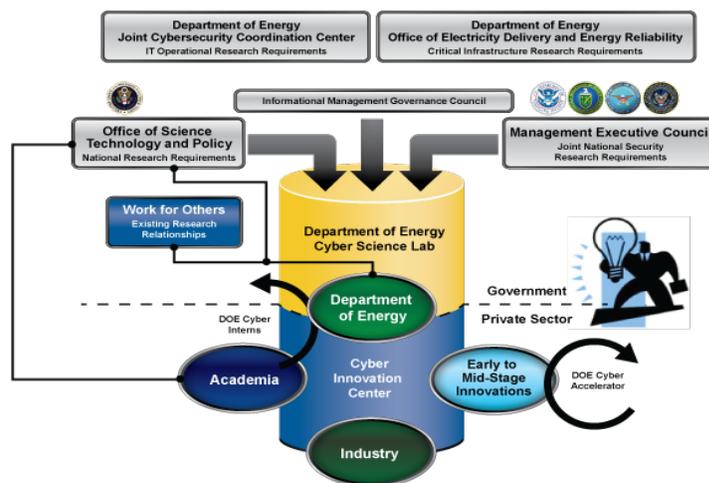
Advance – Leverage the national laboratories’ world class research and development capabilities through the cornerstone of the Cyber Sciences Laboratory (CSL). CSL is a virtual research and development (R&D) center that combines the capabilities of our National Laboratories, academia, and industry to push the theoretical bounds of cyber defense, funnel new capabilities into our infrastructure, and provide an effective mechanism for sharing across government agencies to improve the overall cyber posture for the nation.

9. Establish and Advance the Cyber Sciences Laboratory and Establish a Cyber Innovation Center

The CSL will establish and sustain an enduring, national cybersecurity R&D center of excellence at the National Laboratories to address cybersecurity threats to the nuclear deterrent, energy infrastructure, and the nation's reliance on cyber infrastructure at large. It creates a new set of structures and processes that bring our capabilities together in a way that improves the efficient use of government-wide resources and improves the transition of cutting edge cyber technologies into DOE/NNSA's own operational environment. The Cyber Innovation Center will be modeled on other successful DOE Innovation Hubs and will work closely with the private sector, academia and in particular with early to mid-stage innovators (similar to DoD Cyber Accelerator Program) to accelerate national progress in cybersecurity technology and operations.

10. Engage and Leverage the Best of Government, Industry, Academia and Innovators

This tenth and final objective improves the effectiveness and efficiency of modernization efforts by establishing structures and processes that establish and sustain collaborative relationships with the best of government, industry, academia and innovators. It creates a mechanism to discover, evaluate and implement best practices and insertion-ready technologies in an appropriately secure environment.



Each of these ten strategic objectives requires unity of effort across the Department's business, mission and functional leadership. Achieving these objectives will result in more effective and agile IT services and potentially will require fewer people and financial resources to deliver

them. The importance of governance, transparency of data and process, and continuous vertical and horizontal communication cannot be overstated.

CURRENT IT MODERNIZATION ACTIVITIES

PortfolioStat

On March 30, 2012, Acting Director of the Office of Management and Budget (OMB), Jeffrey Zients, directed Heads of Executive Departments and Agencies to implement a [PortfolioStat process](#) to: (1) submit an action plan to consolidate the commodity IT spend under the CIO, and establish a measurable financial goal to reduce total IT spend based on more consolidated commodity IT buys and intra-agency shared services by June 29; and (2) to complete and submit to OMB a document outlining its plan to rationalize and consolidate its IT portfolio, including the adoption of intra- and inter-agency shared IT services by August 31. All Program and Staff Offices are represented and collaborating in the PortfolioStat process via their ITC representatives.

The Deputy Secretary presented DOE's strategy to OMB on August 22, 2012. DOE/NNSA's ongoing efforts are expected to yield at least \$10 million/year in savings and cost avoidance, and save a total of \$75 million from FY 2010 to FY 2015.

DOE CIO/NNSA "RightPath to IT Transformation"

RightPath was jointly established by the DOE and NNSA CIOs to deliver an efficient and modernized IT infrastructure that enables a virtual workforce where employees may work anywhere, anytime, from any device while enhancing collaboration, business intelligence, and the agency's cybersecurity posture by combining transformative changes in people, processes, and technology. These capabilities provide for leaner government, improve employee satisfaction and retention, enhance the agency's cyber security posture, improve energy efficiency, and reduce long-term infrastructure needs for housing employees.

RightPath will modernize the infrastructure, improve the cybersecurity posture, and deliver service with lower operational costs. This transformation will be accomplished by constructing the IT toolbox for the 21st century that integrates and leverages disruptive technology trends of the future, such as cloud computing, mobility, social computing, and big data/analytics. Through RightPath, DOE and NNSA are focusing this enterprise approach on non-differentiated Federal IT (i.e., those underlying and foundational systems and services that do not differentiate Program and Staff Offices from each other). Examples include: core desktop computing, storage, and connectivity provided by datacenters and server rooms; mainframes/servers; telecommunications; desktop systems; mobile devices; email; non-email collaboration tools; identity access and management; corporate cybersecurity services; and web hosting infrastructure.

RightPath leverages the best innovations of the private sector and the DOE/NNSA National Laboratories and other M&O contractors. The resultant system will be agile, lean, integrated, shareable, and flexible to enable the full or partial integration of DOE/NNSA site architectures as appropriate for the mission and as an enabler to maximizing fiscal efficiency. RightPath is initially focused on delivering urgently needed capabilities to NNSA, which will also serve to pilot enterprise effectiveness and efficiency improvements.

RightPath includes the following core components:

- **YOURcloud** – Secure, hybrid, community cloud, broker-based services on the Infrastructure on Demand (IoD) capability in place at Los Alamos National Laboratory (LANL) and managed and deployed by a commercial cloud solution provider with IoD serving as the broker, orchestration, and security envelope.
- **OneNNSA Network** – A secure, mesh, wide-area network connecting all NNSA sites, along with providing secure, broad network access to YOURcloud services that can leverage DOENET or other connections.
- **ONEvoice** – A unified communications capability available to all DOE CIO/NNSA users that combines email, instant messaging, web conferencing, desktop sharing, video conferencing, and Voice over Internet Protocol (VoIP) phone services.

RightPath provides a foundation for other commodity IT modernization efforts. As services are rolled out, the OCIO will broker those services for the entire Department. As they mature and are proven scalable, these capabilities will be delivered to other Program Offices as part of implementing the broader overall IT strategy.

Office of Science's IT Modernization Project

The Office of Science's (SC) Information Technology Modernization Project (ITMP) will modernize the SC infrastructure, deliver service at reduced operating costs, improve cyber security, and provide new technologies to enhance collaboration and mobile computing. The SC ITMP vision will maintain a federated organizational approach to IT for SC, but establish a Senior Information Officer (SIO) at headquarters to be the SC single point of contact of IT matters; enable SC information to be accessible to those that need it, when they need it and where they need it; and, comprises people, technology, and processes reflecting industry-standard management practices and efficient use of resources. The SC ITMP aligns with, complements, and supports the tenets of the Department's overall IT Modernization Strategy.

- **Transform:** SC ITMP will transform the SC network by providing secure and robust connectivity to all SC federal sites, very similar to the OneNNSA Network vision. Data centers will be consolidated to leverage existing IT assets and reduce operating costs, energy consumption, and duplicative investments in IT services. Acquisitions and commodity IT services such as email, desktop support, and collaboration

services will be consolidated as a result of the data center consolidation. New technologies such as virtual desktop, bring your own device (BYOD), and public and private cloud computing will be utilized. SC ITMP will leverage existing cloud offerings such as YOURCloud, Google Apps, Microsoft Office 365, or other cloud offerings for commodity IT services based on mission need and business cases developed to support the investments.

The SC ITMP will transform its acquisition process by consolidating IT support service contracts and hardware and software purchases. The transformed acquisition process will be governed by the SC governance structure being established as part of the SC ITMP.

- **Governance:** SC ITMP establishes an Office of Science IT governance structure consisting of an IT Investment Review Board (IRB), IT Steering Committee and SC IT executive. The governance structure will be setting the strategic direction for SC IT investments and reduce duplicative and costly IT services. The SC federated organizational approach to IT will create a centralized approach to policy, direction, standards, architecture and methodologies, but will retain the benefits of having local decision-making in regard to implementation and support.
- **Strengthen Cyber Security:** SC ITMP will establish common cyber security policies and FISMA reporting. SC will consolidate disparate cyber security assets and leverage JC3 and security offerings provided by the Department's OCIO.

Office of Energy's Information Technology and Data Center Modernization Project

The Office of Energy's Information Technology and Data Center Modernization Project (ITDCMP) will allow the Office of Energy to increase the efficiency and effectiveness in the delivery and management of commodity services to Federal staff and support service contractors. The Office of Energy's ITDCMP will focus attention on transforming the IT infrastructure through a more robust service delivery model that consolidates data centers, increases the use of virtual services and reduces operating costs among its five programs: Fossil Energy (FE); Energy Efficiency & Renewal Energy (EERE); Electricity Delivery & Energy Reliability (OE); Nuclear Energy (NE); and Indian Energy Policy & Programs (IE).

Currently, all Office of Energy programs at headquarters leverage commodity IT products and services from the OCIO service catalogue. Where practicable, the Office of Energy will continue to leverage the OCIO's IT broker-advisor model to utilize shared services for its field offices as part of its ITDCMP.

The Office of Energy supports the Department's IT governance framework to include participation in the ITC, and supports many of the cross program ITC working groups in multiple

areas including Enterprise Architecture, Cybersecurity, and Records Management. In addition, the Office of Energy's executive leadership is deeply involved with the Department's IMGCC, the principal governance board for IT and cybersecurity. The goal is to enable common practices in the management, delivery and security of IT services, where applicable, across DOE programs.

- **Transform:** The Office of Energy will continue to support the Department's Sustainability Plan to drive down the use of inefficient IT products, create more robust and virtual data centers and by default decrease green house emissions. The Office of Energy is currently working to consolidate two disparate data centers into one best-of-breed highly efficient data center which has the potential to become a model for other DOE programs. In addition, DOE, through the work performed by EERE, is partnering with industry to develop a Data Center Energy Practitioner (DCEP) program to accelerate energy savings in the dynamic and energy-intensive marketplace of data centers.
- **Protect:** In the realm of cyber security and information assurance, the Office of Energy will leverage the Department's centrally managed core common cyber security policies and FISMA reporting and continues to support the Department's plan towards JC3.
- **Advance:** The Office of Energy will leverage the Department's CSL to address cybersecurity threats to the nuclear deterrent, energy infrastructure, and the nation's reliance on cyber infrastructure at large.

Office of Environmental Management's IT Modernization Project

The Office of Environmental Management (EM) is embarking on a major initiative to improve service provisioning for its sites, while at the same time looking for ways to reduce costs due to tightening budgets. Since the early 1990s, EM has partnered with the Department to consolidate commonly used and shared IT resources. As DOE explores strategic opportunities to leverage existing IT and to foster new and emerging IT to maximize mission accomplishment in a cost effective way, EM's goal is to collaborate with the Department in identifying complementary solutions.

Under its own Collaborative Cloud Initiative, EM will leverage existing Platform as a Service (PaaS) and Software as a Service (SaaS) capabilities at its sites to host voice services and commonly used business applications for collaboration, emergency notification, mobile device management, and enterprise mission systems. These services will take advantage of existing secure multi-tenant DOE infrastructure resources to maximize cost recovery. As more EM sites opt-in to use these services, overall costs to EM are reduced, while the quality and reliability of user experiences increase.

EM is also leading the way in leveraging an innovative public-private partnership through the Department's Energy Saving Performance Contract (ESPC) to achieve commodity IT goals. Working side-by-side with the Federal Energy Management Program (FEMP) contractor, EM is fully engaged in the process to review each EM site and develop a path forward.

The potential savings from the ESPC will come from the consolidation and upgrade of EM's existing infrastructure and the reduction in the operational costs across EM, allowing for better quality of service delivery to our customers. Implementation of the Investment Grade Audit (IGA) recommendation is scheduled to begin in November 2012.

Office of Legacy Management's IT Modernization Project

The Office of Legacy Management (LM) fully supports and is an active participant in many of the Department's strategic objectives. LM utilizes the Enterprise Identity Management System for identity, credential, and access management (ICAM) and has been attending regular meetings to discuss Consolidated Homeland Security Presidential Directive (HSPD)-12, Federal Public Key Infrastructure (PKI), and E-Authentication initiatives. Representatives from LM participated in the PKI TechStat session held by the DOE OCIO in FY 2011. Opportunities for increased efficiencies were identified, including the recommendation to migrate the PKI program to the cloud by 2012. LM is participating in the PKI migration and the eCPIC migration effort to support the transformation to cloud initiatives.

LM employees communicate with the JC3 to improve cybersecurity incident response, reporting, and tracking. LM's participation results in timely and effective routine and urgent communication channels that enhance information sharing for cybersecurity incidents. Additionally, LM requires annual cybersecurity awareness training for its Federal and contractor staff. This effort improves overall cybersecurity effectiveness and reduces cybersecurity incident response costs by reducing the number and seriousness of avoidable incidents. LM is participating in the PortfolioStat process to support the Department's efforts to consolidate its IT portfolio, including the adoption of intra- and inter-agency shared IT services.

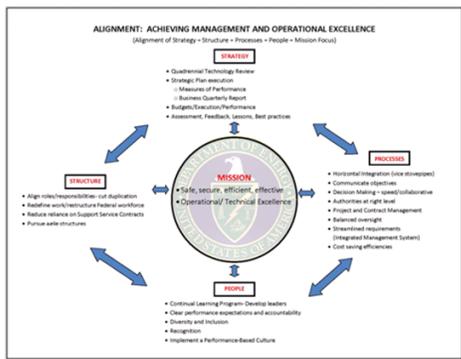
In order to eliminate wasteful spending and better respond to the growing digital communications demands of the 21st century, the Office of Public Affairs is spearheading an effort to create a centralized online platform, via Energy.gov. LM is collaborating with Public Affairs on the Web Renewal project to move the LM Public Website to the Energy.gov domain, so that the stakeholders of the Department can go to one website and locate the information they need on the various offices within the DOE.

CONCLUSION

A commitment to a unified DOE/NNSA approach to IT modernization will deliver foundational improvements in the enterprise that will enable shared services, reduce the cost of IT infrastructure, improve the speed and flexibility of operations, and create the foundation for a

virtual workforce for the 21st century. Program and functional leaders (i.e., Chief Operating Officers and Directors of Functional Offices) will ensure vertical alignment within their organizations and will work collaboratively with the DOE and NNSA CIOs to execute this strategy for the good of the entire Department. Leaders across the DOE/NNSA will embrace and champion the cultural transformation necessary to support the technical, management, organizational and operational changes driven by this strategy.

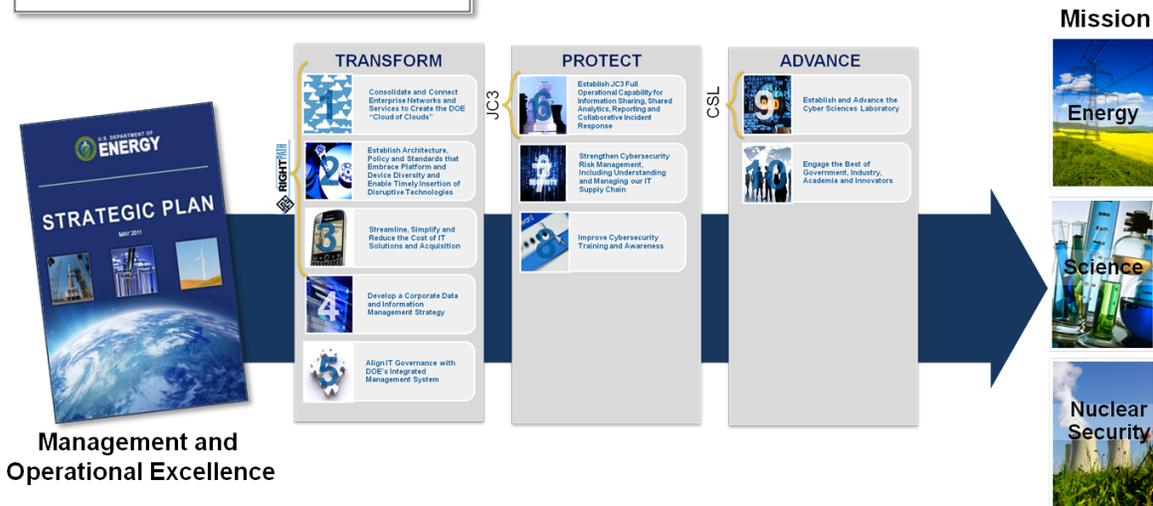
Simultaneously with RightPath and other initiatives, related activities must be championed and led. Today, these are assigned to various working groups, including DOE OCIO/NNSA RightPath IPTs, the DOE OCIO's Corporate IT Project Management Office (PMO) and ITC working groups. Specific initiatives that require integration include sustainability and datacenter consolidation (including ongoing ESPC activities), ICAM, PKI, and network modernization and Internet Protocol Version 6 (IPv6) transition.



Enterprise Risk Management

| | | Impact | | | |
|-------------|----------|------------|----------|-------------|-------------|
| | | Negligible | Low | Medium | High |
| Probability | Certain | Minor | Moderate | Extreme | Extreme |
| | Likely | Minor | Moderate | Significant | Extreme |
| | Possible | Minor | Moderate | Significant | Extreme |
| | Unlikely | Minor | Moderate | Moderate | Significant |
| | Rare | Minor | Minor | Minor | Moderate |

- Minor – risk acceptance may be preferred
- Moderate – existing controls may be adequate
- Significant – may need to add more controls
- Extreme – more controls likely needed



DOE policies and directives must be developed or updated to establish the expectations and requirements for our future IT ecosystem. There is a significant gap across government in policies and standards and the experience of the DOE/NNSA National Laboratories and other M&O contractors is key to future DOE/NNSA and broader U.S. Government success.

STRATEGY OWNERSHIP

The DOE CIO and NNSA CIO are unified in this strategy and are responsible for the coordinated execution of its goals and existing IT governance processes. The CIOs will ensure that program and functional leaders are engaged and informed throughout its execution.

_____/s/_____/ 09/07/2012
Thomas P. D'Agostino (Date)
Under Secretary for Nuclear Security &
Administrator, National Nuclear Security Administration
National Nuclear Security Administration

_____/s/_____/ 09/07/2012
David Sandalow (Date)
Under Secretary of Energy (Acting) &
Assistant Secretary for Policy & International Affairs
Department of Energy

_____/s/_____/ 09/07/2012
Dr. William Brinkman (Date)
Director, Office of Science
Department of Energy

_____/s/_____/ 09/07/2012
Robert F. Brese (Date)
Chief Information Officer
Department of Energy