



Office of the Associate Administrator for Information  
Management and Chief Information Officer

# Implementation Plan



2012-2016

## Message from the Administrator



President Obama has reshaped our national security priorities making enterprise infrastructure modernization with integrated Information Technology (IT) capabilities a key strategic initiative. Our IT infrastructure must ensure that our workforce can access appropriate information in a secure, reliable, and cost-effective manner. Effective information sharing throughout the government enhances the national security of the United States (US). For the National Nuclear Security Administration (NNSA), effective information sharing helps strengthen our nuclear security mission; builds collaborative networks within NNSA as well as with the Department of Energy (DOE), Department of Defense (DoD), and other national security components; improves the foundation, speed, and execution of decision making; and helps improve the ability to anticipate events and resource needs. This Implementation Plan is being issued to provide direction to NNSA's information sharing and modernization efforts by detailing goals and objectives necessary to build a strong IT infrastructure.

Every individual and organization within NNSA will play an important role in improving our IT environment. Successful implementation of this strategy will result in efficiencies of operation, enhanced and shared operational awareness, and mission success. I look forward to working with each of you on this important initiative to achieve "OneNNSA."

Thomas P. D'Agostino  
Administrator, National Nuclear Security Administration

## Message from the Associate Administrator for Information Management and Chief Information Officer



I am pleased to present the NNSA Information Management Implementation Plan, which codifies our vision for providing an enhanced computing environment and increased cyber security posture today, while looking forward towards meeting tomorrow's technology and challenges.

Transforming NNSA from keepers of the Nuclear Weapons Complex to a fully integrated Nuclear Security Enterprise (NSE) requires that information be viewed as a strategic asset and force multiplier.

We will be investing in cutting edge information technology and teaming with the best and brightest people in order to ensure that we deliver our desired collaborative capabilities and cyber security posture in support of "OneNNSA."

I look forward to working with each of you as we achieve the goals set forth in this plan.

Robert J. Osborn, II  
Associate Administrator for Information Management and Chief Information Officer,  
National Nuclear Security Administration

# TABLE OF CONTENTS

<b>EXECUTIVE SUMMARY .....</b>	<b>III</b>
<b>INTRODUCTION .....</b>	<b>1</b>
OVERVIEW .....	1
STRATEGIC GOALS.....	2
NNSA NETWORK VISION (2NV) STRATEGY BACKGROUND.....	2
STAKEHOLDERS.....	3
<b>INFORMATION MANAGEMENT STRATEGIC GOALS .....</b>	<b>4</b>
<b>FOCUS AREA 1: ENCHANCING OUR CAPABILITIES .....</b>	<b>4</b>
<i>Strategic Goal 1-1: Collapse and Consolidate Networks, Applications, and Services into Virtualized Environments .....</i>	<i>4</i>
<i>Strategic Goal 1-2: Build the Next Generation Mobile Infrastructure .....</i>	<i>4</i>
<i>Strategic Goal 1-3: Leverage the Power of the Cloud to Enable a Low Cost, Shared Services Model .....</i>	<i>5</i>
<i>Strategic Goal 1-4: Establish Risk-Based Cyber Security Governance .....</i>	<i>5</i>
<i>Strategic Goal 1-5: Improve Business Processes .....</i>	<i>6</i>
<b>FOCUS AREA 2: UNDERSTANDING OUR ENVIRONMENT .....</b>	<b>7</b>
<i>Strategic Goal 2-1: Provide Real-Time Situational Awareness of NNSA Networks and Systems.....</i>	<i>7</i>
<i>Strategic Goal 2-2: Operationalize Research in Next Generation Cyber Security Defenses .....</i>	<i>7</i>
<i>Strategic Goal 2-3: Improve Cyber Security Incident Management Capabilities.....</i>	<i>8</i>
<i>Strategic Goal 2-4: Provide Continuous Monitoring Capabilities for NNSA Networks and Systems .....</i>	<i>8</i>
<b>FOCUS AREA 3: PROTECTING OUR FUTURE.....</b>	<b>9</b>
<i>Strategic Goal 3-1: Invest in Cutting Edge Research on Cyber Security Defenses .....</i>	<i>9</i>
<i>Strategic Goal 3-2: Apply Risk-Based Budgeting Processes for Cyber Security .....</i>	<i>9</i>
<i>Strategic Goal 3-3: Improve Stakeholder Involvement in NNSA IT Programs .....</i>	<i>10</i>
<i>Strategic Goal 3-4: Develop an Enterprise Governance Process for IT Investments.....</i>	<i>10</i>
<b>ENVIRONMENT, CONTEXT, AND ALIGNMENT .....</b>	<b>11</b>
<b>STRATEGIC PILLARS.....</b>	<b>12</b>
NNSA NETWORK VISION (2NV) .....	13
JOINT CYBERSECURITY COORDINATION CENTER (JC3) .....	15
CYBER SCIENCES LABORATORY (CSL).....	15
<b>STRATEGIC INITIATIVES.....</b>	<b>17</b>
CONGRESSIONAL AND OFFICE OF MANAGEMENT AND BUDGET (OMB) ENGAGEMENT .....	17
CONTINUOUS MONITORING.....	17
CYBER SECURITY RISK MANAGEMENT FRAMEWORK .....	18
ENTERPRISE SECURE NETWORK (ESN) .....	18
ENTERPRISE WIRELESS .....	18
EXECUTION AND GOVERNANCE MODEL FOR INFORMATION TECHNOLOGY (EGMIT).....	19



IMPROVED ACQUISITION AND SUPPLY CHAIN .....	20
<b>THE PATH FORWARD .....</b>	<b>21</b>
<b>APPENDIX A: ACRONYMS .....</b>	<b>22</b>

## LIST OF FIGURES

FIGURE 1: OMB MEMORANDUM FOR CIO AUTHORITIES .....	1
FIGURE 2: THREE STRATEGIC PILLARS .....	12
FIGURE 3: 2NV “CLOUD OF CLOUDS” .....	13
FIGURE 4: 2NV CONCEPTUAL ARCHITECTURE BY SERVICE LAYERS .....	14
FIGURE 5: JC3 PROGRAM .....	15
FIGURE 6: CSL PROGRAM .....	15
FIGURE 7: ESN PROJECT .....	18
FIGURE 8: NOTIONAL WIRELESS ARCHITECTURE .....	19
FIGURE 9: ENTERPRISE GOVERNANCE MODEL .....	19

## LIST OF TABLES

TABLE 1: FOCUS AREA MAP TO STRATEGIC INITIATIVES.....	2
TABLE 2: ALIGNMENT BETWEEN 25 POINT IMPLEMENTATION PLAN AND STRATEGIC INITIATIVES .....	3
TABLE 3: ALIGNMENT TO DOE AND NNSA STRATEGIC PLANS .....	11

# EXECUTIVE SUMMARY

## **Associate Administrator for Information Management and Chief Information Officer's Intent**

Our focus for the next five years is to transform the NNSA computing environment in support of the Administrator's "OneNNSA" vision. We will accomplish this by delivering three pillars of our strategy: the NNSA Network Vision (2NV), the Joint Cybersecurity Coordination Center (JC3) and the Cyber Sciences Laboratory (CSL). 2NV will enhance and modernize our current environment by providing a secure, mobile, agile and adaptive IT infrastructure which will allow our workforce to perform their duties from any device, anywhere, at any time. JC3 will allow us to understand the "health" of that computing environment from a cyber security and network operations perspective. CSL will provide research and development capabilities which will ensure our future ability to achieve the NNSA mission. We will develop and use a comprehensive Enterprise Architecture (EA) to guide our path towards achieving our end state, and will manage investments towards that achievement via a structured enterprise governance process.

## **Vision**

We will provide a secure, mobile, agile, device agnostic computing environment which supports the needs of the NNSA now and into the future.

## **Mission**

The mission of the NNSA Associate Administrator for Information Management and Chief Information Officer (CIO) is to provide state of the art communications technology and services which support the NNSA lines of business, in the most efficient manner possible, with a resulting increase in cyber security posture.

## **Strategic Goals**

To achieve the "OneNNSA" vision, the NNSA Office of the Associate Administrator for Information Management and Chief Information Officer (OCIO) has developed three strategic focus areas along with supporting goals and initiatives to be accomplished within the next five years using light technologies and best practices to provide enterprise-wide services in a cost effective and efficient manner.

# INTRODUCTION

## Overview

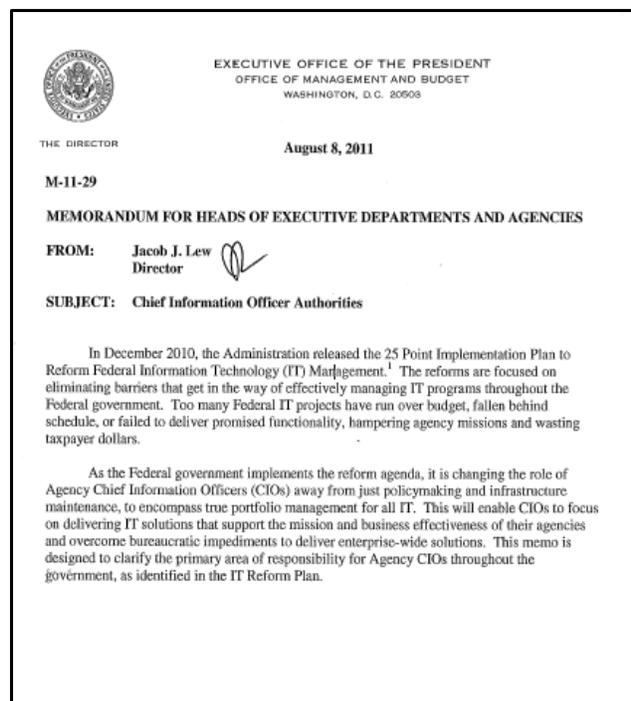
The NNSA Information Management Implementation Plan provides a roadmap for the future of NNSA Information Technology (IT) and cyber security within the context of the broader NNSA Network Vision (2NV). The NNSA Office of the Associate Administrator for Information Management and Chief Information Officer (OCIO) has the responsibility to manage assured information collaboratively within the Nuclear Security Enterprise (NSE) as a key enabler and transformational agent that ensures program, operational and business excellence in the accomplishment of the NNSA mission in a safe, secure, and efficient manner.

## Changes in the Role of the Chief Information Officer

In December 2010, the Administration released the 25 Point Implementation Plan to Reform Federal Information Technology Management (25 Point Implementation Plan). The 25 Point Implementation Plan focuses on eliminating barriers that get in the way of effectively managing IT programs throughout the Federal government. Furthermore, in August 2011, the Office of Management and Budget (OMB) released M-11-29, Chief Information Officer Authorities, to re-emphasize the initiatives of the 25 Point Implementation Plan and the changes in the role of Chief Information Officers (CIOs) from just policymaking and infrastructure maintenance, to encompass true portfolio management for all IT. In addition to their statutory responsibilities through the Clinger-Cohen Act and related laws, CIOs are now empowered to improve the operating efficiency of their Agencies by having a lead role in the following four business functions:

1. Governance
2. Commodity IT
3. Program Management
4. Information Security

Agency CIOs will be held accountable for lowering operational costs, terminating and turning around troubled projects, and delivering meaningful functionality at a faster rate while enhancing the security of information systems. These additional responsibilities will enable CIOs to reduce the number of wasteful duplicative systems, simplify services for the American people, and deliver more effective IT to support their Agency's mission.



**Figure 1: OMB Memorandum for CIO Authorities**

## Strategic Goals

To achieve the NNSA Administrator’s “OneNNSA” vision and support the 25 Point Implementation Plan, the NNSA OCIO has developed a set of strategic focus areas, strategic goals, and strategic initiatives, integrated through the 2NV strategy, to accomplish within the next five years using light technologies and best practices to provide enterprise-wide services in a cost effective and efficient manner.

**Table 1: Focus Area Map to Strategic Initiatives**

Focus Area	Goals	<u>Pillars/Initiatives</u>
Enhancing Our Capabilities	<ul style="list-style-type: none"> <li>• Consolidation</li> <li>• Mobility</li> <li>• Cloud Computing</li> <li>• Risk Management</li> <li>• Business Process Management</li> </ul>	<ul style="list-style-type: none"> <li>• <b><u>NNSA Network Vision (2NV)</u></b></li> <li>• Enterprise Wireless</li> <li>• Risk Management Framework (RMF)</li> <li>• Enterprise Secure Network (ESN)</li> <li>• Improved Acquisition &amp; Supply Chain</li> </ul>
Understanding Our Environment	<ul style="list-style-type: none"> <li>• Situational Awareness</li> <li>• Operationalizing Research</li> <li>• Incident Management</li> <li>• Continuous Monitoring</li> </ul>	<ul style="list-style-type: none"> <li>• <b><u>Joint Cybersecurity Coordination Center (JC3)</u></b></li> <li>• Continuous Monitoring</li> </ul>
Protecting Our Future	<ul style="list-style-type: none"> <li>• Investment in Cyber Defense Research</li> <li>• Risk-Based Budgeting</li> <li>• Stakeholder Involvement</li> <li>• Governance</li> </ul>	<ul style="list-style-type: none"> <li>• <b><u>Cyber Sciences Laboratory (CSL)</u></b></li> <li>• Congressional and Office of Management and Budget (OMB) Engagement</li> <li>• Execution and Governance Model for Information Technology (EGMIT)</li> </ul>

## NNSA Network Vision (2NV) Strategy Background

The current IT resources are located within the NNSA Headquarters (HQ), three national laboratories, four production sites, and the National Nuclear Security Site (NNSS). Each site is geographically distributed and represents approximately \$2 billion in IT capital assets. Current IT investments are stove piped and not standardized across the enterprise. Costs to maintain current IT investments translate into postponement of mission work. IT labor and data costs are replicated significantly to support multiple infrastructures, multiple networks, and excess legacy data centers.

The 2NV strategy, in concert with the other strategic pillars, such as JC3 and CSL, will transform NNSA into a leading Federal organization that aggressively pursues the initiatives in the 25 Point Implementation Plan.

**Table 2: Alignment between 25 Point Implementation Plan and Strategic Initiatives**

OMB Initiative	NNSA Implementation
Shift to a “Cloud First” policy	Collection of private clouds will provide initial shared services, and policy updates will make cloud solutions the preferred alternative for future IT projects.
Identify 3 Must Move Cloud Services	2NV will move email, web conferencing, instant messaging, and web portals into the cloud during the first phase.
Reduce the Number of Federal Data Centers	Deployment of private clouds will facilitate the retirement of legacy data centers as applications and systems are transitioned. In addition, 2NV will leverage commercial data centers instead of building and managing independent Federal data centers.
Improving IT Project Execution	The Execution and Governance Model for Information Technology (EGMIT) will allow project management requirements to be specifically tailored for IT success instead of leveraging a common process with construction projects. The approach will deliver projects faster, in smaller chunks, and with an improved portfolio management process.
Deliver Infrastructure as a Service (IaaS) solution	IaaS will enable NNSA to transition to a standard virtualized desktop for improved security and lower cost of ownership.
Develop a Strategy for Shared Services	The CSL can further increase the attractiveness of Department of Energy (DOE) investments by providing a central mechanism for sharing results (where appropriate) amongst all of the participating Agencies. The sharing concept ensures each Agency sees the result from all government investments; not just their own. In addition, the CSL will directly feed research results into DOE through the JC3.

Ultimately, the strategic initiatives will transform the Administration’s IT infrastructure into an interconnected, agile, secure, and efficient computing environment for the NSE. The NNSA strategy tackles the full spectrum of issues facing our IT/Cyber programs by delivering an integrated and secure NNSA “cloud” architecture. It achieves efficiency by reducing redundancy and it increases effectiveness and security through an integrated architecture that focuses on shared services, virtualized environments, and mobile architectures.

## Stakeholders

Enterprise stakeholders are both our customers and strategic partners. Both are critical to our mission. They include:

- Department of Defense (DoD)
- Department of Energy (DOE)
- Department of Homeland Security (DHS)
- Department of State (DoS)
- Industry
- Intelligence Community
- Interagency Partners
- Management and Operating (M&O) Contractors
- Multi-national Organizations
- Non-DoD US Federal Agencies
- United Kingdom
- The American people

# INFORMATION MANAGEMENT STRATEGIC GOALS

## FOCUS AREA 1: ENHANCING OUR CAPABILITIES

### **Strategic Goal 1-1: Collapse and Consolidate Networks, Applications, and Services into Virtualized Environments**

Individual services are being maintained by Headquarters, labs, and plants that essentially perform the same function. These services require site data storage and administration, infrastructure, and software. Where this common service exists across sites, these need to be identified and migrated to a virtualized service solution. This will provide standardization and reduce maintenance efforts while enabling all customers to benefit at the same time from future upgrades or enhancements.

#### **Strategic Goal 1-1 Objectives:**

- Leverage National Security Agency (NSA) Suite B technology to replace the majority of existing classified networks and machines (ability to go high-side from the green environment).
- Leverage Voice over IP (VOIP) technology to replace the majority of NSE stand-alone voice systems.
- Apply an enterprise architecture approach to redesign the NNSA unclassified networks into one integrated NSE network.
- Consolidate data centers throughout the NSE to reduce energy, labor, and hardware costs.
- Apply an aggressive virtualization strategy to minimize hardware and labor requirements for IT systems.

### **Strategic Goal 1-2: Build the Next Generation Mobile Infrastructure**

Mobile computing is a versatile and potentially strategic technology that improves information quality and accessibility. Mobile technology is also a great enabler of shared IT services and can reduce IT costs. It reduces the need for distributed IT resources while allowing centralized computing that can be more robust and efficient. Additionally, mobile technology improves operational efficiency by allowing the worker to create, access, process, store and communicate information without being constrained to a single location. Within the NNSA environment, this must be implemented without any adverse impact to security.

#### **Strategic Goal 1-2 Objectives:**

- Transition to secure wireless technology as the preferred approach for last-mile connectivity throughout the NSE (indoor and outdoor).
- Leverage NSA Suite B solutions to develop a classified wireless capability for the NSE.
- Invest in secure mobile solutions for next generation platforms to move beyond the Blackberry.
- Build secure, wireless sensor and Radio Frequency Identification (RFID) networks to eliminate and/or optimize manual labor processes.

### **Strategic Goal 1-3: Leverage the Power of the Cloud to Enable a Low Cost, Shared Services Model**

After implementation, cloud computing will provide low cost software on a large scale, with advanced security in a homogeneous or common environment. It provides on demand access from anywhere and will allow resources to be pooled. In addition, as the infrastructure, platforms, and software are migrated to the cloud, better business intelligence or analytics will be achieved; clouds for the labs, the plants, and headquarters can be constructed to optimize resources.

#### **Strategic Goal 1-3 Objectives:**

- Implement a secure Federal cloud for shared services.
- Implement a secure Laboratory cloud for shared services.
- Implement a secure Plant cloud for shared services.
- Implement an external collaboration cloud for interacting with vendors, review teams, and other stakeholders.
- Federate identities and presences between clouds and mirror them for disaster recovery/fail-over.
- Bring secure web conferencing and unified communications to every desktop in the NSE.
- Invest in rich, interactive collaboration experiences for executive communications.
- Provide NSE employees with the ability to work securely in the unclassified environment from anywhere with an internet connection.

### **Strategic Goal 1-4: Establish Risk-Based Cyber Security Governance**

The importance of cyber security standards and their application within NNSA cannot be overstated. To deliver the NNSA mission, a robust vulnerability and risk management solution will continuously discover and prioritize network exposures. A cyber security governance framework will ensure adherence and compliance with applicable standards. This framework will enable NNSA to achieve the following cyber security strategic goals: 1) Organize for unity of purpose and speed of action; 2) Enable secure-mission driven access to information and services; 3) Anticipate and prevent successful attacks on data and networks; and 4) Prepare for and operate through cyber degradation or attack. Policies will be in place to support and enable the 2NV strategy. The cyber security framework will include provisions for a standardized system Certification and Accreditation (C&A) and leveraging enterprise or site level plans and assessments to reduce paperwork.

#### **Strategic Goal 1-4 Objectives:**

- Transition NNSA policy to a Risk Management Framework (RMF) that reduces spending on compliance activities and redirects spending into technical controls and direct mitigation.
- Improve cyber Research and Development (R&D) by leveraging the Cyber Sciences Lab (CSL) Program.
- Improve incident response and situational awareness by leveraging the capabilities of the Joint Cybersecurity Coordination Center (JC3).
- Invest in rich analytics, forensic capabilities, and incident response to combat the high end, advanced persistent threat.
- Invest in the continuing education of our cyber security professionals to ensure that they are equipped with the knowledge to combat the most sophisticated threats.

## Strategic Goal 1-5: Improve Business Processes

An enterprise governance framework and decision making body will ensure consistent IT spending to support the 2NV strategy and provide services in a virtualized environment. The ability to replace disparate services with common shared services from a cloud will enhance NNSA capabilities, while allowing better resource allocation within the enterprise.

This work is a primary endeavor of the NNSA Conceptual Architecture. Faithful implementation of the conceptual architecture will result in an interconnected, agile, secure, and efficient network. A primary focus of the conceptual architecture will be to provide guidance for implementation of an integrated and secure NNSA cloud infrastructure that, in turn, provides access to enterprise common services. Doing so will result in a corresponding reduction in technical redundancy with increased business process effectiveness and security. Finally, the architecture will provide context and guidance for development of a more effective business intelligence/analytics capability. The conceptual architecture aligns with the goals and objectives of the “OneNNSA” outcome: NNSA will realize significant efficiencies and provide leadership within the Federal sector by bringing “first of kind” capabilities to the NSE. The 2NV strategy will also realize greater coordination and collaboration within the NSE, while reducing the need for redundant Federal data centers and provide a significant cost savings to the Administration.

### **Strategic Goal 1-5 Objectives:**

- Institutionalize a cyber security and software quality assurance reciprocity process to eliminate/minimize rework at each site.
- Transition to a “One Function, One System” philosophy for common, shared services within the NSE.
- Invest in platform solutions to address a broad spectrum of needs versus point solutions for specific problems. Leverage the enterprise platforms to retire legacy systems.
- Develop an agile and robust system integration approach (i.e. Enterprise Service Bus) to allow for the secure exchange of data between systems.
- Leverage cloud security for NNSA email communications.
- Transition towards modular procurements.
- Align acquisition and budget submittal processes.

## FOCUS AREA 2: UNDERSTANDING OUR ENVIRONMENT

### **Strategic Goal 2-1: Provide Real-Time Situational Awareness of NNSA Networks and Systems**

Individual networks, sites, and systems are currently monitored by multiple, redundant, and independent Security Operations Centers (SOCs). NNSA will collapse these capabilities into one state of the art SOC via JC3 to improve real-time situational awareness, to understand the full operating picture across all environments, and to dramatically improve communications on cyber related issues.

#### **Strategic Goal 2-1 Objectives:**

- Collapse stand-alone capabilities in the classified environment, unclassified environment, and intelligence arena into one state of the art SOC via JC3.

### **Strategic Goal 2-2: Operationalize Research in Next Generation Cyber Security Defenses**

The JC3 will have the capability to understand the state of NNSA networks, in real-time, including any potential weak areas that may need enhancement. The JC3 will provide the demand-side of the equation of JC3 as the DOE/NNSA input to CSL for cyber defense research and development focus areas. Once developed, JC3 will rapidly deploy these new capabilities within DOE/NNSA production networks and systems.

#### **Strategic Goal 2-2 Objectives:**

- Leverage insight provided by situational awareness capabilities to feed need areas for cyber research to CSL.
- Rapidly deploy new technology from the CSL into NNSA production networks and systems.

### **Strategic Goal 2-3: Improve Cyber Security Incident Management Capabilities**

The JC3 will have the capability to rapidly deploy a geographically dispersed cadre of highly capable cyber security professionals to assist a site with handling high impact incidents. Information related to incidents will be rapidly shared to prevent the spread of cyber attacks.

#### **Strategic Goal 2-3 Objectives:**

- Develop a dedicated cadre of geographically dispersed and highly capable cyber security professionals to respond rapidly to major incidents and requests for assistance.
- Maintain a catalog of cyber security capabilities at each site to assist with incident response.
- Rapidly share incident related information to minimize the effect of cyber attacks.

### **Strategic Goal 2-4: Provide Continuous Monitoring Capabilities for NNSA Networks and Systems**

The JC3 will apply a graded approach to continuous monitoring that centralizes logs from a distributed architecture of sensors into the enterprise monitoring systems.

The JC3 will invest in enterprise class tools for analyzing large amounts of sensory data, transforming and normalizing data, and then providing business intelligence capabilities that identify trends and anomalous behavior on NNSA networks. Information will be made available to NNSA leadership, and access controlled through the 2NV portal.

#### **Strategic Goal 2-4 Objectives:**

- Provide a graded approach to continuous monitoring that provides real-time capabilities to the most sensitive assets and leverages the RMF to appropriately apply monitoring to other assets based on the consequence of loss and the probability of attack.
- Provide a central monitoring capability via JC3 that federates monitoring logs from each of the sites.
- Invest in rich analytic tools to provide cyber security related business intelligence that identifies trends and anomalous behavior.
- Provide a centralized SOC dashboard within the 2NV portal.

## FOCUS AREA 3: PROTECTING OUR FUTURE

### **Strategic Goal 3-1: Invest in Cutting Edge Research on Cyber Security Defenses**

In the current operating environment, research is primarily funded by external national security related agencies and is not shared within the current operating environment. Through the Cyber Sciences Laboratory (CSL), NNSA will make investments in game changing cyber defenses through the application of research and development and scientific discovery processes. Promising research will be funneled back through JC3 for operationalization.

#### **Strategic Goal 3-1 Objectives:**

- Invest in game changing technologies that will fundamentally improve NNSA cyber security defenses.
- Serve as the pre-eminent cyber security defense laboratory in the U.S. government and leverage unique NNSA capabilities to improve cyber security defenses across multiple cabinet level Agencies.
- Develop a virtual, cloud-based cyber range capability for advanced simulation and testing.

### **Strategic Goal 3-2: Apply Risk-Based Budgeting Processes for Cyber Security**

As the capabilities of the Advanced Persistent Threat (APT) continue to increase, it is imperative that NNSA optimize the cyber security budget using a risk-based process. Development of a common baseline, coupled with deployment of the RMF at each site, should ensure that the highest priority initiatives in cyber security are effectively funded.

#### **Strategic Goal 3-2 Objectives:**

- Develop a baseline set of metrics and performance expectations for NNSA cyber security programs.
- Leverage the RMF at each site to identify issues needing additional funding beyond the baseline capabilities.
- Ensure that each additional dollar invested in cyber security programs maximizes risk reduction for sensitive NNSA information.

### **Strategic Goal 3-3: Improve Stakeholder Involvement in NNSA IT Programs**

In order to ensure the long-term health of the NNSA IT program, the OCIO must strengthen the partnership with the DOE OCIO to leverage true enterprise platforms where appropriate. In addition, pro-active communication with congressional bodies and OMB is necessary to ensure that funding is available to meet NNSA priorities. Finally, industry partnerships must be established to ensure the most efficient and effective technologies are rapidly deployed within NNSA.

#### **Strategic Goal 3-3 Objectives:**

- Strengthen the partnership with the DOE Chief Information Officer Office to leverage true enterprise platforms where appropriate.
- Actively engage congressional bodies and OMB on the NNSA OCIO strategy, investments, and priorities.
- Strengthen partnerships with industry to ensure that the most efficient and effective technologies are deployed.

### **Strategic Goal 3-4: Develop an Enterprise Governance Process for IT Investments**

Current IT investments within NNSA are loosely controlled at best. The OCIO will establish an enterprise governance process that ensures stakeholder involvement and proper alignment of IT projects for all new Federal IT initiatives and major M&O IT projects. The process will establish clear roles and responsibilities for IT projects and ensure alignment with the NNSA Enterprise Architecture.

#### **Strategic Goal 3-4 Objectives:**

- Establish an enterprise governance process that ensures stakeholder involvement in “green lighting” new IT projects.
- Establish clear roles and responsibilities for the lifecycle management of IT projects.
- Ensure that new IT projects fit within the NNSA Enterprise Architecture.

# ENVIRONMENT, CONTEXT, AND ALIGNMENT

Considerable effort is being placed in assuring alignment between the NNSA Information Management Implementation Plan and the NNSA Strategic Plan, taking into consideration the relationships and context inherited through the overarching Department of Energy (DOE) Strategic Plan. The NNSA OCIO will strive for congruence with the NNSA Administrator’s Key Goals, the NNSA Operating Principles and Goal 3 of the DOE Strategic Plan as shown below.

**Table 3: Alignment to DOE and NNSA Strategic Plans**

	<b>NNSA Strategic Goals &amp; Operating Principles</b>	<b>NNSA OCIO Strategic Goals</b>
<b>DOE Strategic Goal #3: Enhance nuclear security through defense, nonproliferation, and environmental efforts.</b>	<ul style="list-style-type: none"> <li>• Modernize the NNSA infrastructure.                             <ul style="list-style-type: none"> <li>○ We will shape the infrastructure to assure we have the core capabilities necessary to execute our mission responsibilities and create a 21st century Nuclear Security Enterprise.</li> </ul> </li> <li>• We will also modernize our IT infrastructure to ensure that our workforces can access appropriate information in a secure, reliable, and cost effective manner.</li> </ul>	<ul style="list-style-type: none"> <li>• Build the Next Generation Mobile Infrastructure</li> <li>• Leverage Cloud Computing to Enable a Low-Cost Shared Services Model</li> <li>• Provide Situational Awareness</li> <li>• Operationalize Research</li> <li>• Provide Incident Management</li> <li>• Perform Continuous Monitoring</li> </ul>
	<ul style="list-style-type: none"> <li>• Strengthen the science, technology, and engineering base.</li> </ul>	<ul style="list-style-type: none"> <li>• Invest in Cutting Edge Research on Cyber Security Defenses</li> </ul>
	<ul style="list-style-type: none"> <li>• Drive an integrated and effective enterprise.                             <ul style="list-style-type: none"> <li>○ We will use more effective governance and business models.                                     <ul style="list-style-type: none"> <li>• We will improve our NNSA-wide governance to drive the concept of “OneNNSA”. Decisions will take into account the requirements of all elements of our enterprise, eliminating internal stovepipes within the NNSA. We will use risk-informed Federal oversight models that clarify roles and responsibilities and eliminate non-value added oversight activities. Our enterprise partners will have greater flexibility, without compromising accountability, to realize cost savings and to further operational effectiveness. We will actively capture best practices in industry and across the enterprise to solve problems more effectively and efficiently.</li> </ul> </li> </ul> </li> <li>• We succeed only through teamwork, innovation and continuous improvement.</li> <li>• We will pursue our mission such that management, staff, and processes are integrated across and exchanged freely within the NNSA.</li> </ul>	<ul style="list-style-type: none"> <li>• Invest in Cyber Defense Research</li> <li>• Collapse and Consolidate Networks, Applications, and Services into Virtualized Environments</li> <li>• Improve Business Processes</li> </ul>
	<ul style="list-style-type: none"> <li>• Our Mission is vital and urgent – we must constantly focus on mission outcomes.</li> <li>• We pursue our mission in a manner that is safe, secure, legally and ethically sound, and fiscally and environmentally responsible.</li> <li>• We manage risk across the program objectives and operational performance to fulfill our mission.</li> <li>• We apply validated standards and rely on rigorous peer reviews.</li> </ul>	<ul style="list-style-type: none"> <li>• Establish Risk-Based Governance</li> <li>• Develop an Enterprise Governance Process for IT Investments</li> <li>• Perform Risk-Based Budgeting</li> <li>• Promote Stakeholder Involvement</li> </ul>

# STRATEGIC PILLARS

The future IT environment will implement an agile approach which will be intrinsically capable of delivering enterprise services and solutions to better meet the NNSA business needs. While there are a number of issues facing the NNSA IT and cyber programs, the outcome will be an integrated and secure architecture that achieves efficiency and increases effectiveness through a Service-Oriented Architecture (SOA). The NNSA OCIO plans to implement the future IT environment through key initiatives centered on three strategic pillars: the NNSA Network Vision (2NV), the Joint Cybersecurity Coordination Center (JC3) and the Cyber Sciences Laboratory (CSL).



**Figure 2: Three Strategic Pillars**

Enterprise governance, enabled by the three principle pillars, will advance the concept of “OneNNSA” by eliminating internal stove pipes and identifying enterprise risks using holistic measures and risk-informed models. These models will be employed to clarify roles and responsibilities. The result will enable NNSA enterprise partners to have greater flexibility, without compromising accountability, and it will enable them to realize cost savings and operational effectiveness. The future infrastructure will be smaller and will deliver more value as NNSA transitions to an integrated and secure NNSA “cloud” architecture. In alignment with the NNSA Strategic Plan, the OCIO will execute these goals and actions to employ “a management approach that integrates leadership, people, and processes to better accomplish our goals as a unified Nuclear Security Enterprise.”

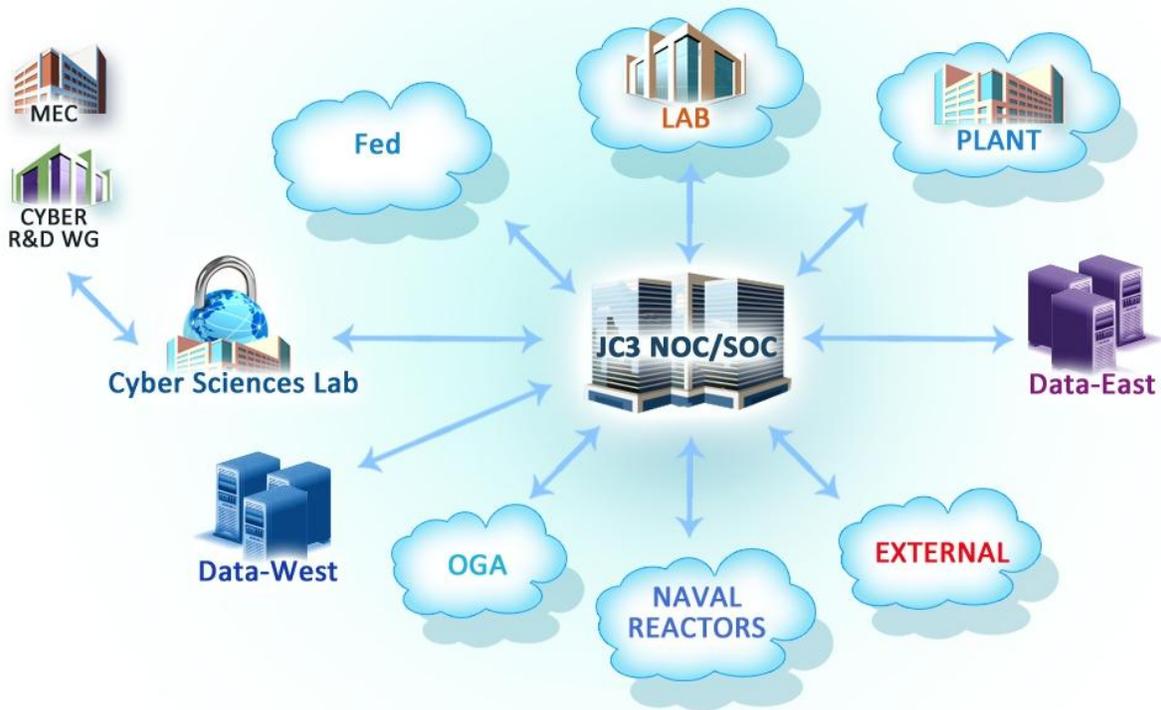


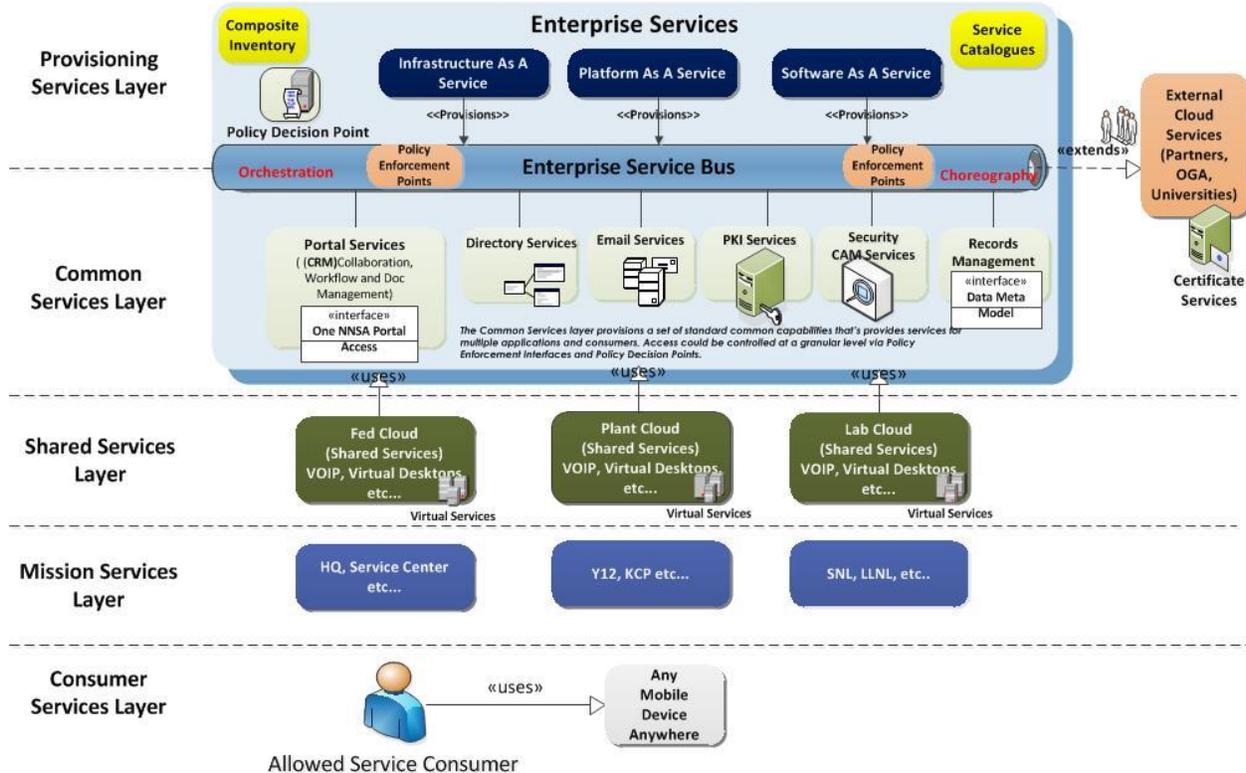
Figure 3: 2NV “Cloud of Clouds”

## NNSA Network Vision (2NV)

2NV will enhance and modernize our current environment by providing a secure, mobile, agile and adaptive IT infrastructure which will allow our workforce to perform their duties from any device, anywhere, at any time. The figure below depicts the interrelationships between the OCIO’s mission, goals, vision, and outcomes supported by the culture to achieve the “OneNNSA.” The NNSA OCIO prescriptive architecture envisions a cloud architecture that provides common services so that Headquarters, sites, labs, and plants can decrease backlog mission critical work and align with the 2NV strategy. Consistent with the 2NV, some examples of potential common services will include: email, web conferencing, collaboration, high performance computing, emergency response management, records management, facilities management, etc.

# NNSA Notional Network Vision

## Conceptual Architecture



**Figure 4: 2NV Conceptual Architecture by Service Layers**

Implementation of this architecture will result in greater coordination and collaboration among participants in information management policy and technology deployment. An enhanced risk management process will promote improved decision making in program, operations, and business activities. This will result in greater productivity and will reduce costs within a transformed NSE, in support of the NNSA and the Federal inter-agency national security community.

The 2NV architecture will provide an integrated and secure NNSA cloud and result in an interconnected, agile, secure, and efficient network. At the same time, there will be a corresponding reduction in the redundancy of applications, networks and services that will increase both effectiveness and security.

The collaborative culture resulting from 2NV implementation will enable more efficient use of IT investments and more rapid access of IT services. Collaborative behavior, a core value of "OneNNSA", is necessary to achieve program, operational and business excellence for mission success in a safe, secure and efficient manner. NNSA will achieve the "We operate jointly" culture needed to support governance policy to optimize success and, ultimately, to excel at what we do.

## Joint Cybersecurity Coordination Center (JC3)

Incident management reform is a key element of the DOE Secretary's Management Excellence Initiatives. In the spring of 2010, the Department conducted an assessment of its Incident Management Program to improve its agility, efficiency, and efficacy. The assessment identified the need for an Incident Management and Response Program that: 1) provides agile, robust, transparent, and integrated capabilities for the DOE front-line cyber security operations; 2) utilizes the collective DOE expertise; and 3) meets Federal requirements for incident management and response. The JC3 was formed in 2011 to achieve these objectives.

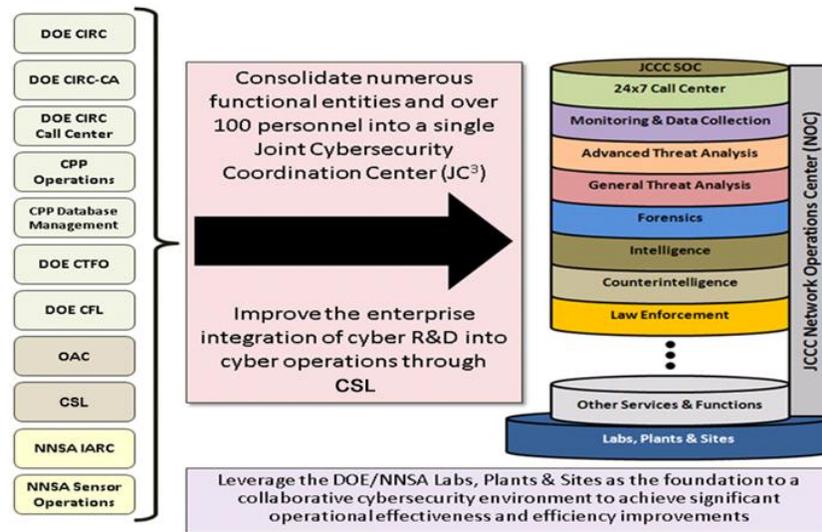


Figure 5: JC3 Program

The JC3, which includes NNSA engagement, will allow the Department to understand the "health" of its computing environment from a cyber security and network operations perspective. The JC3 will be responsible for consolidating the cyber security incident management capability and governance processes into a single comprehensive unit, streamlining information sharing, reporting, and access to technical resources (24 hours a day, 7 days a week), while preserving individual participant organization's unique requirements and information.

## Cyber Sciences Laboratory (CSL)

The United States' (U.S.) military, economic, and social fabrics have become inextricably dependent on an IT infrastructure that is inherently insecure. A National level effort, on the scale of the Manhattan Project, is necessary to ensure that our critical infrastructure and most precious information is resilient against the broad range of threats presented by malicious hackers, terrorists, and foreign nations.

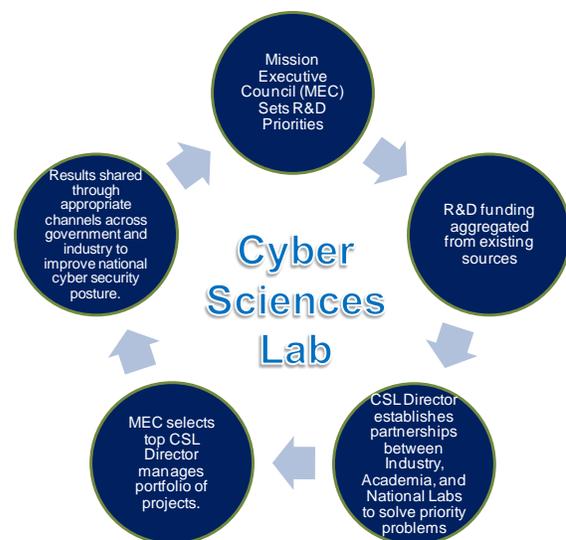


Figure 6: CSL Program

DOE is taking the challenge of leading the CSL Program, as it is the single Federal Agency where world class science meets an urgent national security mission.

The CSL Program provides a framework to focus currently fragmented investments towards the most critical cyber security R&D needs; ensure mitigations and solutions are shared in a timely manner; and foster collaboration with industry to ensure critical infrastructure is “born secure” in the future, and with academia to ensure we continue to have talented and skilled cyber warriors.

The CSL Program consists of the following five key elements:

1. Mission Executive Council (MEC) governance board ensures the highest national priorities are addressed by the CSL Program.
2. Aggregating funding lowers the costs to each individual sponsor while increasing net R&D results.
3. Research and results will be shared among partners as appropriate to improve the national cyber security posture.
4. Industry partnership allows solutions to be applied during development and manufacturing in order to lower future cyber security operational costs.
5. Academic partnerships inform universities of future workforce needs.

# STRATEGIC INITIATIVES

The following strategic initiatives, centered on our three principle pillars, show how IT modernization is providing enterprise-wide cost efficiencies and progress toward achieving “OneNNSA” while aligning with the Information Management strategic goals.

## **Congressional and Office of Management and Budget (OMB) Engagement**

The NNSA Administrator and the Associate Administrator for Information Management and Chief Information Officer will proactively engage with Congress and OMB on the strategy, value and required investments for the NNSA 2NV. Through this proactive engagement, the NNSA will develop a partnership of purpose and an assurance of accountability for performance.

The required resources for 2NV will be clearly communicated by means of a distinct line-item budget for IT/Cyber programs. The line-item budget is devolved and implemented through Multi-Year Program Plans and Annual Program Implementation Plans. These plans will specify performance targets that the NNSA will monitor and report on progress in order to improve mission performance. Through the demonstrated success in IT/Cyber infrastructure modernization and operations, NNSA will validate their initial and sustained commitment of the 2NV to Congress and OMB.

## **Continuous Monitoring**

The NNSA depends on information systems to carry out its missions and business functions. The NNSA information systems are subject to serious threats that can have adverse effects on organizational operations (e.g., missions, functions, and reputation), organizational assets, individuals, other organizations, and the Nation by compromising the confidentiality, integrity, or availability of information processed, stored, or transmitted by those systems. Consequently, NNSA cyber security is evolving from a compliance-based and artifact-centric approach to an Automated Continuous Monitoring risk-based mission methodology.

Automated Continuous Monitoring is the necessary solution to address the security impacts to the NSE resulting from changes to hardware, software, firmware, or operational environment. The adoption of a well-designed and well-managed continuous monitoring solution will transform the NNSA’s static, compliance-based risk determination process into a dynamic process. It will also enable essential, time-sensitive security information to reach organizational officials within a timely manner, allowing the appropriate cost-effective, risk-based decisions regarding the operation of the NSE. Specifically, Automated Continuous Monitoring will integrate information security more closely into the NNSA Enterprise Architecture (EA) and System Development Life Cycle (SDLC); promote near real-time risk management and ongoing system authorization through the implementation of robust continuous monitoring processes; and provide senior leaders with the necessary information needed to make risk-based decisions regarding the NSE, in support of their core missions and business functions.

## Cyber Security Risk Management Framework

Because of the NNSA mission, the NNSA OCIO has established a risk-based approach to cyber security. Based on the NNSA Policy (NAP) 14.1D, "NNSA Cyber Security Policy/Framework," the NNSA Program Cyber Security Plan (PCSP) includes provisions for systems' C&A, while leveraging enterprise or site level plans and assessments to reduce paperwork. The RMF will transition NNSA from a compliance-focused approach to cyber security, to a real-time, configuration management, situational awareness-focused program that pro-actively identifies and mitigates threats.

## Enterprise Secure Network (ESN)

ESN is a project sponsored by NNSA to facilitate the secure exchange of classified information and capabilities across the NSE. ESN consists of independent site installations of standardized equipment and Commercial off-the-Shelf (COTS) software that are integrated through a common infrastructure, and shared policies and procedures. ESN is currently deployed at all NNSA sites, multiple DOE sites, other departments and organizations, and select allied nations. There are additional sites being integrated and limited-access gateways under development and construction.

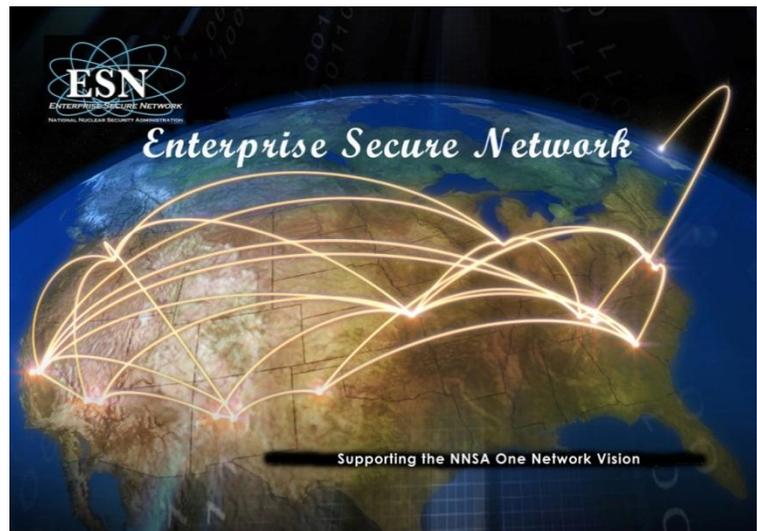
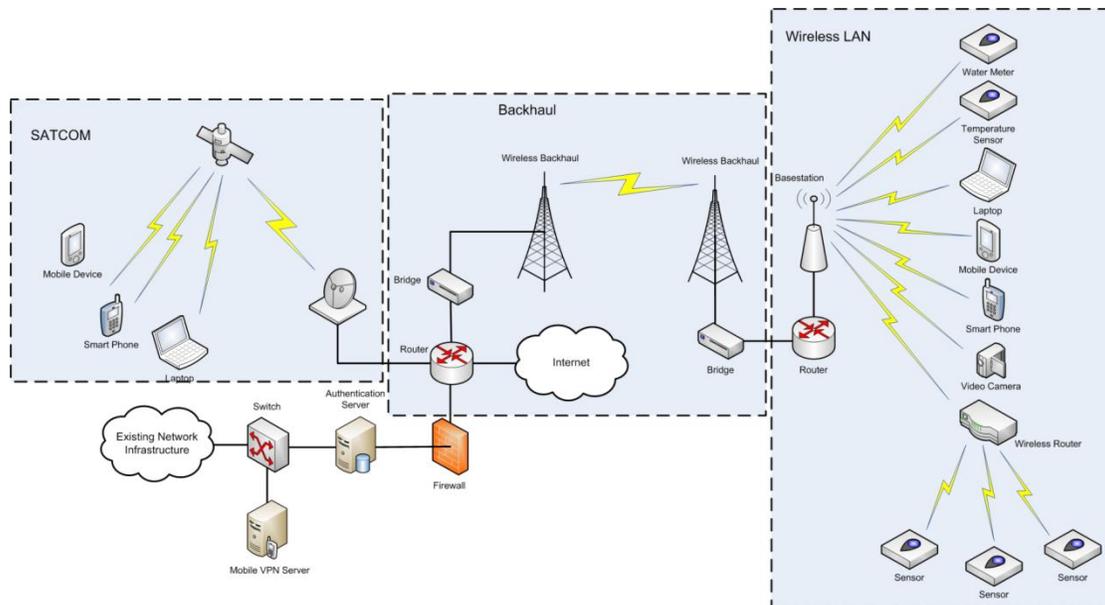


Figure 7: ESN Project

## Enterprise Wireless

In support of the NNSA mission elements, each site produces and utilizes massive amounts of information and data that are used for both mission execution and operations support in the unclassified and classified environments. The transmission of this information and data is primarily accomplished between sites (both intra- and inter-site) through wired data networks. While these networks have served the weapons complex well for many years, they inherently limit the transformation of the complex into a more agile and integrated enterprise. Connectivity to the wired network is limited by physical network drops, vastly limiting the flexibility of facility use, the mobility of its workers, and the overall agility of the enterprise to adapt to evolving technology and mission scope. The NSE Wireless Project will implement a pervasive wireless network capability that will greatly improve the responsiveness and efficiency of the NSE as part of its overall infrastructure recapitalization. The NSE Wireless Project will:

- Develop a process to implement secure wireless infrastructure across the NSE.
- Deliver a wireless-fabric infrastructure to enable new application scenarios throughout the NSE.
- Leverage other funding sources to serve as a force multiplier for magnifying the benefits of infrastructure investments.



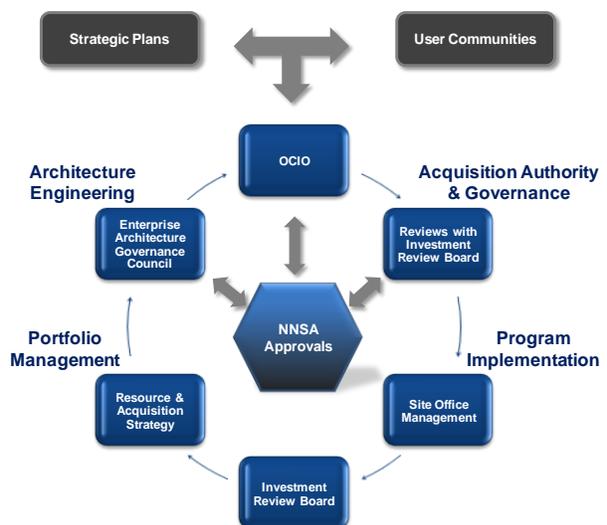
**Figure 8: Notional Wireless Architecture**

## Execution and Governance Model for Information Technology (EGMIT)

Enterprise Governance is the set of responsibilities and practices exercised by the governance bodies with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the organization’s resources are used responsibly. Enterprise Governance integrates EA governance and IT governance into one model for the management and oversight of capital assets. Enterprise Governance is implemented through the EGMIT.

The purpose of the EGMIT is to provide a foundation and supporting structure, designed to aid in the acquisition and management of IT investments within the NSE. The EGMIT, which replaces the IT requirements of DOE Order (O) 413.3A, *Program and Project Management for the Acquisition of Capital Assets*, is based on industry best practices that are specifically tailored to improve the execution of NNSA IT investments and projects. It covers the entire life cycle of an IT investment (from initial planning to final retirement or decommission) with the flexibility to be tailored toward IT investments

varying in project size, complexity, scope, duration, iterative development methodologies, and other unique factors. This phased and systematic approach is a proven government and industry method for reducing risk and achieving more effective and efficient results from invested resources. The ultimate utility for the Project Manager (PM) and the operational end-users is better-constructed IT



**Figure 9: Enterprise Governance Model**

applications, services, or shared infrastructure. These, in turn, will lead to predictable and effective delivery of NNSA capabilities. The requirements of the EGMIT map directly to the requirements of the TechStat, one of the key initiatives outlined in the 25 Point Implementation Plan. The TechStat, administered by OMB, is a face-to-face, evidence-based accountability review of an IT investment, which results in concrete actions to address weaknesses and turn around troubled investments.

## **Improved Acquisition and Supply Chain**

The Federal Acquisition Streamlining Act (FASA) of 1994 requires IT projects to streamline procurements to fast track IT investments. Based on the 25 Point Implementation Plan, IT acquisitions can provide significant savings while providing capabilities faster to the enterprise. eSourcing and eStores can be placed in a cloud and the enterprise can achieve standardization and cost efficiencies, while lowering costs to maintain current infrastructure.

# THE PATH FORWARD

The Information Management Implementation Plan establishes the goals and key initiatives for the NNSA IT/Cyber community and demonstrates how they align with the overall NNSA Strategic Plan to deliver effective solutions. All of the work performed should support one or more strategic goals and objectives. This alignment ensures that NNSA is using our limited resources to satisfy our strategic goals in an agile and efficient manner. We will update the implementation plan routinely to incorporate new technologies and best practices. It will also serve as a way of transparently communicating the direction and scope of our goals and objectives to our stakeholders. This will allow us to better align our resources with the NNSA's mission.

Separate Implementation Plans will be prepared for each strategic initiative to support this high level plan. The plans will report on the progress and milestones accomplished, and will be updated as new initiatives are introduced or when existing initiatives are completed. Additionally, a Communications Plan will be developed and maintained to define the target audiences, key messages that are trying to be articulated, frequency of communication, desired outcomes, communication vehicles, and senders.

# APPENDIX A: ACRONYMS

ACRONYM	DEFINITION
2NV	NNSA Network Vision
APT	Advanced Persistent Threat
C&A	Certification & Accreditation
CIO	Chief Information Officer
COTS	Commercial Off-the-Shelf
CSL	Cyber Sciences Laboratory
DHS	Department of Homeland Security
DoD	Department of Defense
DOE	Department of Energy
DoS	Department of State
EA	Enterprise Architecture
EGMIT	Execution and Governance Model for Information Technology
ESN	Enterprise Secure Network
FASA	Federal Acquisition Streamlining Act of 1994
IT	Information Technology
JC3	Joint Cybersecurity Coordination Center
M&O	Management & Operating
MEC	Mission Executive Council
NAP	NNSA Policy
NNSA	National Nuclear Security Administration
NNSS	National Nuclear Security Site
NSA	National Security Agency
NSE	Nuclear Secure Enterprise
O	DOE Order
OCIO	Office of the Associate Administrator for Information Management and Chief Information Officer
OMB	Office of Management and Budget
PM	Project Manager
R&D	Research & Development
RFID	Radio Frequency Identification
RMF	Risk Management Framework
SDLC	System Development Life Cycle
SOA	Service Oriented Architecture
SOC	Security Operations Center
US	United States



