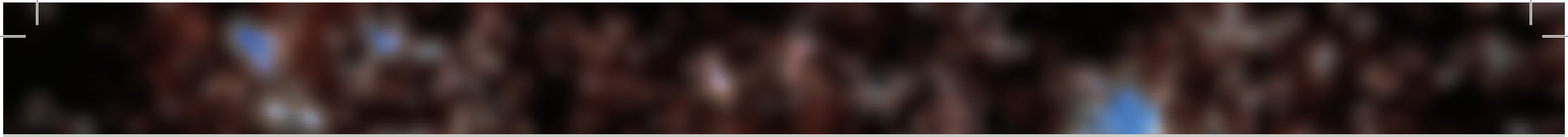

The Enterprise Secure Network Project

Rich Tannich, NNSA OCIO;
Thomas M. Boorman, HPC-5

ESN is a project sponsored by the NNSA to facilitate the secure exchange of classified information and capabilities across the Nuclear Security Enterprise and with collaborating agencies. ESN consists of independent site installations of standardized equipment and COTS software that are integrated through a common infrastructure and share policies and procedures. ESN features an Enterprise identity model, strong authentication, and centralized monitoring and analysis capability. ESN is currently deployed at all NNSA and multiple DOE sites. There are additional sites being integrated, including limited access gateways and international sites.

Fig. 1. ESN was honored as one of the 10 GCN Honorable Mention Awards for Information Technology Achievement in Government for 2010. NNSA Administrator Thomas D'Agostino says: "The Enterprise Secure Network is not only critical to the security of our nuclear weapons program, but to our efforts to transform the Cold War nuclear weapons complex to a 21st-century national security enterprise."

To provide an Information Technology (IT) solution to enable the Nation's nuclear weapons stockpile and supporting infrastructure to be more responsive to the threats of the 21st century, the National Nuclear Security Administration (NNSA) established the Enterprise Secure Network (ESN) and designed a business and risk-based approach to accomplish the mission.

In the past several years, ESN leaders and project teams have designed and built substantial improvements in secure communications and collaboration, cross-site workflow, two-factor authentication, network management, application integration, and single sign-on among the various laboratories and plants within the national security enterprise (NSE). When it became operational 2 years ago, ESN solved a long-standing problem: the NNSA's difficulty in sharing classified data. ESN has built on the success of its initial rollout by adding innovative capabilities, transactions, services, and processes that greatly increased efficiency and enhanced its ability to fulfill this critical mission (see Fig. 1).

Project leaders and engineering teams employed a risk-based management approach and worked closely with NNSA management to perform the following tasks:

- Extended the ESN collaborative domain by establishing agreements for interagency and international collaborations
- Based on stakeholder requirements, developed a new centralized architecture component that implements a "small site hub" capability, enabling ESN enterprise support of sites with small user populations and limited resources
- Implemented additional connectivity options at sites, including limited-access gateways to collaborating agencies, "light" (non-redundant) sites, and "connection-only" sites
- Integrated a significant number of ESN-enabled applications that allow secure cross-complex data sharing and collaboration using Web-based and legacy applications
- Implemented and deployed a "basic fileshare" core service, which allows ESN users to securely share classified information across the complex
- Added classified and unclassified Web conferencing capabilities to enable interactive, real-time information sharing and discussions
- Developed an effective new workflow-based and management-focused trouble ticket tracking system to support customer needs
- Grew the user population to nearly 1000 users

Another key factor in the successful development of ESN is ongoing efforts by the NNSA leadership to foster a culture of cooperation and collaboration among a large number of historically independent – and even competitive – commercial sites and laboratories. ESN now routinely convenes multisite teams, meetings, and projects with representation from the Department of Energy (DOE), NNSA, Department of Defense (DoD), and international organizations and agencies.

Due to the sensitive nature of nuclear-related information and operations, ESN operates in a high-risk environment. Historically, federal management approaches have been risk averse. However, the NNSA believes that such risk aversion may impede the daily functions of an organization, and lead to nonstandard configurations of hardware, software, and services within the NSE. In 2010, ESN designed a standardized set of core configurations to be deployed at all new sites, substantially improvingd technology refresh, maintenance, operator training, and system operations. These configurations make ESN operations more secure, effective, and cost efficient. ESN now consists

For more information contact Thomas M. Boorman at tmb@lanl.gov

of 15 independent sites spanning nine states—and, later this year, two continents—using standardized equipment, procedures, and core services with a variety of applications (see Fig. 2). By utilizing industry standards, NNSA best practices, and tailored commercial off-the-shelf (COTS) products, ESN has developed a stable, scalable infrastructure that will meet the stringent security requirements of NNSA sites and collaborating agencies. Primary sites (those with significant user populations and application hosting), such as SNL and LANL, feature redundancy in critical components with automatic failover. ESN has been designed for high availability and reliability so that the scientists and engineers at plants across the US can accomplish their mission confident that the ESN will provide secure communications and collaboration.

Fig. 2. ESN sites across the globe.

ESN employs a standard security assertion markup language (SAML) to implement the authentication and authorization infrastructure. It also features strong two-factor authentication using RSA SecurID tokens. The majority of this work is performed with indigenous talent: architecture, engineering, operations, and project team members hail from representative sites. There are also teams of trained subject matter experts (SME) who spearhead technology development, deployment, and troubleshooting efforts at local or remote sites. The training and utilization of ESN SMEs also allows them to become local resources who enhance technical expertise at their respective sites.

The expanded cyber security and functionality of ESN have substantially improved the ability of DOE and NNSA to work effectively and share data and resources across the NSE as they manage the nuclear weapons stockpile. As new sites, cooperating agencies, and international facilities are integrated, ESN greatly enhances their ability to share critical information and respond effectively to situations and emerging threats.

New web collaboration tools have increased cooperation and collaboration among developers and customers, and the multisite nature of ESN also improves the level of cooperation and coordination between participating sites and agencies. A shared ESN development environment, hosted at LLNL, allows multisite teams to work together on the design, development, and testing of new services and applications. Hundreds of ESN users added over the past year can now cooperate and collaborate to a degree never before possible on any classified network. As these shared resources become available to a wider set of authorized users, ESN has greatly enhanced security and reliability, using a standardized approach and around-the-clock monitoring and helpdesk availability. The application of earned value metrics helps ensure that work is tracked and managed appropriately.

In cooperation with the Product Realization Integrated Digital Enterprise (PRIDE) organization, the growing availability of shared legacy applications on the ESN has transformed the ability of the NNSA and cooperating agencies to leverage existing external applications and share resources and expertise. Additionally, the network operations center has prevented any cyber intrusions into the network or infrastructure.

Due to the past year's significant ESN team accomplishments, DOE and NNSA have made tremendous operational advances. Cost savings have increased due to cross-site data sharing and cooperative services such as the enterprise-level Oracle purchase. Organizational agility has increased due to the integration of 10 PRIDE applications and recent connectivity of ORNL and PNNL. Cost effectiveness will increase by the end of the year as the DoD Secret Internet Protocol Router Network (SIPRNet) and United Kingdom gateways are completed. HPC Division supports and helps guide these efforts by providing resources not only for the operations of ESN but also by providing one-of-a-kind technology developed at LANL, such as the advanced context sensitive filter efforts needed for the gateways. Due to ESN's efforts a new approach to writing nuclear policy is available now that the connection is finalized with the White House Office of Science and Technology Policy (OSTP) at the New Executive Office Building.

These new tools, services, and appreciation for data sharing have ushered in a new culture of cooperation and coordination. Additionally, these factors support the Administration's goal of transforming the Nation's nuclear weapons stockpile and supporting infrastructure to increase responsiveness to the threats of the 21st century.

Funding Acknowledgments
National Nuclear Security Administration