



**System 1, Inc.
Expression of Interest for Sandia National
Laboratory**



**6701 Democracy Blvd., Suite 300
Bethesda, Maryland 20817**

Small Business

POC: John M. Abeles
Telephone: 301-214-9077 Office
301-792-4581 Mobil
Email: jabeles@syst1.com

Web Presence: www.syst1.com



Summary of System 1 Expertise

System 1 is a small business specializing in strategic and tactical cybersecurity solutions for effective security, privacy, and critical infrastructure protection programs. Our clients include Federal, State, Local and private sector organizations. We are specialists in cultural change and technology. We support the transition to more secure and cost effective environments by changing behavior to integrate security into mission accomplishment. Our primary areas of expertise include:

- Implementation of risk based security programs leading to reduced costs and improved performance
- Adapting security to new technologies – transition to the cloud, mobile security, and telework
- Security simplification, architecture, system consolidation, and continuous monitoring
- Increasing security in a collaborative research and development environment
- Management and governance support for IT Services
- Integration of cyber security, enterprise architecture, capital planning, privacy, and critical infrastructure protection

System 1 personnel continuously meet and exceed our customer's expectations. We can structure a risk-based approach, evaluate your cyber security program posture, and provide proven processes and lessons learned to improve that program. More importantly, we incorporate those processes seamlessly into the culture and mission delivery so they can be cost-effectively maintained. Through cost effective continuous monitoring activities and education, System 1 has shown our customers how security performance can be improved.

We have extensive experience across the Department of Energy and the National laboratories, as well as other Federal Agencies and in the private sector. System 1's expertise has been recognized by the White House, the Secretary of Energy, and was recently appointed by the Attorney General to the Maryland Cyber Security Council.

Our personnel serve as "thought leaders" for contractors and the government. A typical senior System 1 person has 25 years of industry and government support experience. We have a wide variety of backgrounds including management, security, and operations for defense, civilian, and the intelligence communities. Our personnel typically have advanced degrees and certifications. Most of our personnel have a top secret or higher clearance. We are one of the "best in class" small governance and security firms.

Sampling of our Federal Clients

- Department of Commerce
- Department of Education
- Department of Energy
- Department of Interior
- Department of the Treasury
- Environmental Protection Agency
- Intelligence Community
- National Institute of Standards and Technology
- National Parks Service
- National Laboratories
- Security and Exchange Commission
- US Patent and Trademark Office
- White House



Why System 1?

- **System 1 has extensive experience in optimizing governance processes and brokering cost effective solutions** – System 1 has experience optimizing IT frameworks and bridging the gap between theoretical policy and the reality of implementation. System 1 has transitioned organizations from compliance to risk based security. We have formulated and staffed Program Management offices, and have conducted business process engineering to streamline the implementation of new requirements. We have answered the basic question of, “How can one cost effectively and efficiently integrate and manage IT processes?” For example, System 1 has developed an A-130 framework for the Department of Interior. We developed a DOE-wide Site Assist Process and deployed it across the national laboratories in the Office of Science and Office of Environmental Management. We have supported NNSA in the formulation of cloud security and governance, and supported them for external audits. System 1 has performed cultural change, security enhancement, and system consolidation for the Department of Energy.
- **System 1 has experience supporting NIST** – System 1 is a “thought leader” and has a history of developing next generation solutions in the security environment. We have developed special studies for NIST management, SP 800 series documents, NIST interagency reports, and supported NIST and OMB by providing seminars and briefings. We supported the development of the private sector risk management framework and are supporting efforts to formulate information sharing and Analysis Organizations.
- **System 1 has experience in evaluating security maturity and performance in a Federal environment** – System 1 was one of the primary authors of the NIST Program Review for Information Security Management Assistance (PRISMA) framework and the accompanying database. PRISMA provides a repeatable; standards based assessment methodology to determine the maturity level of an organization’s cyber security program. Examples of Federal agencies where System 1 has evaluated security maturity and performance include Federal Emergency Management Agency (within DHS), US Patent and Trademark Commission, Department of the Interior, the Department of Energy, and a number of the contractor operated National Laboratories.

System 1 personnel have also been the primary contributors for other NIST 800 series documents. We have expanded our assessment capability by fielding the DOE development C2M2 assessment model for the energy sector. We have piloted and evolved an IT version of this for the Office of the Chief Information Officer.



- **System 1 understands the importance of effective communication** – System 1 has developed and conducted a wide variety of briefings and presentations that have spanned all levels, from senior leadership to system owners to Congressional presentations and testimony.
- **System 1 understands technology** – We have personnel that perform the Information System Security Officer and Security Engineer roles. We perform risk assessments on new and evolving technologies, and have been supporting the development of new cloud models. We are optimizing the processes and tool sets for continuous monitoring.
- **System 1 understands and has implemented critical infrastructure protection throughout the Federal Government and has supported several States** – System 1 has developed approaches to identifying both physical and cyber assets, and has developed a logical, workable approach to ensure they are appropriately protected. This includes the execution of Project Matrix approaches and interdependency analyses between the Federal Government and the private sector. Metrics, responses to OMB reporting requirements, updates, and support for audits and assessments are included in these approaches. We are also working at the regional level with states, local jurisdictions and the private sector.

System has a current GSA Schedule 70 .

System 1 is an ethics based company – we perform solutions that are meant to improve the quality of life now and in the future.

System 1 Potential Support Areas

System 1 has assessed the Scope of Work and identified where we can support delivery of services to SNL. The areas are listed below:

- **Nuclear Weapons** - System 1 can support cybersecurity and supply chain as a component of nuclear weapons support. We have supported the implementation of cybersecurity and cloud security solutions. We have also developed the DOE requirements for safety of the weapons stockpile going back to Order and 10 CFR 830, as well as performing independent oversight of the management and security of the stockpile.

System 1 can develop and implement streamlined methods to protect information resident on networks, the cloud, and high performance computing systems. We are familiar with and helped develop national and departmental requirements, and implement cost effective solutions.

- **Defense Nuclear Proliferations** – System 1 has experience defining and implementing cybersecurity solutions to ascertain the effectiveness of security regimes and approaches,



to protect valuable information and producte processes in a vulnerable and high threat environment.

- **Science (SC)** – System 1 has directly supported SC on an enterprise level, forming a cybersecurity community and leveraging that to boost performance throughout the National Laboratories. When the Inspector General reviewed the approach and implementation, they recommended that all DOE adopt the approach. On that subject, we have spoken at cybersecurity research conferences sponsor by the labs.
- **Laboratory Management Information Technology (IT) and Cyber Security** – System 1 has been working with the OCIOs in supporting cybersecurity. We recently completed 5 ½ years of a 5 year contract and have been given a bridge contract while the work is being competed. System 1 has completed restructuring of the OCIOs operational environment (AHE) from a flat structure with approximately 120 systems to a tiered approach with approximately 6 enclaves. This has reduced the paperwork and streamlined both the authorization and maintenance processes. Our knowledge and communication with NIST gave us insight that provides strategies and methods to make security more cost effective, and move from a compliance based approach to a more effective risk based approach.

Specific Examples of System 1 Similar Past Performance

System 1 is experienced in the development and implementation of various security approaches for NIST including co-authoring SP 800 series documents, NISTIRs, and special studies for management. We have helped DOE implement the approaches that we developed, as well as supported anumber of Federal Agencies and communities, which provides System 1 personnel with a broad breadth of experience and knowledge. This broad experience allows us to visualize which approaches and solutions will work best in the given circumstances.

NIST, Computer Security Division

System 1 has national policy level experience in cyber security. System 1 personnel has supported NIST in the development of the Federal standards and guidance including NIST SP 800 110, *Information System Security Data Reference Model* and SP 800-65, *Integrating Security into the Capital Planning and Investment Control Process*.

System 1 has experience in both developing a security maturity model for NIST and evaluating security maturity and performance in the Federal environment. System 1 was one of the primary authors of the NIST Program Review for Information Security Management Assistance (PRISMA) framework and the

STANDARDS-RELATED HIGHLIGHTS AT NIST

- ◆ Partnered with NIST on PRISMA, and was one of the authors of NISTIR 7358 and developed database
- ◆ Co-authored NIST SP 800-110.
- ◆ Performed special studies for NIST management.
- ◆ Co-authored NIST 800-65 and presented training/seminars for NIST and OMB.
- ◆ Implement CSEAT (earlier version of PRISMA on FEMA and DOI)



accompanying database. PRISMA was issued in NIST Interagency Report (NISTIR) 7358, *Program Review for Information Security Management Assistance (PRISMA)*, in 2007.

The PRISMA process has been used to meet the continuous monitoring requirements under FISMA and NIST mandates. Examples of Federal agencies where System 1 has evaluated

TA	Management, Operational, and Technical Areas	Policy	Procedures	Implemented	Tested	Integrated
1	Information Security Management & Culture	0.63	0.60	0.30		
2	Information Security Planning	0.20	0.20			
3	Security Awareness, Training, and Education		0.65	0.37	0.31	
4	Budget and Resources		0.40	0.20		
5	Life Cycle Management					
6	Certification and Accreditation	0.80	0.30			
7	Critical Infrastructure Protection		0.60	0.30		
8	Incident and Emergency Response	0.80	0.50			
9	Security Controls	0.80	0.60	0.60		

security maturity and performance includes Federal Emergency Management Agency US Patent and Trademark Commission, Department of the Interior, US Geological Survey, the Department of Energy, and a number of the National Laboratories (focused on advanced scientific research).

System 1 supported NIST’s development of the Risk Management Framework for the government and for the private sector.

Department of Energy, Office of Intelligence and Counterintelligence (DOE-IN)

System 1 is a member of the Transition Guidance Group and is involved in genesis of the 503 standards being proposed. This will bring a level of convergence between NIST standards and guidance, and those being used to protect national security. System 1 is supporting Department of Energy Intelligence and Counterintelligence, and is actively providing comments on the CNSSI 1253 Security Controls Catalog for National Security Systems and CNSSI 1253A, *Guide to Assessing Security Controls for National Security Systems*. In this role we are working with the DOE-IN Senior Agency Information Security Officer to assure that all security documentation includes common artifacts of compliance that can be used to facilitate reciprocity between agencies. We are also working with the Field Intelligence sites within DOE to assure that the FISMA requirements are understood and to integrate security categorization and assessment into the OMB model. We are using the output of this analysis to influence the CNSSI 1237 Managing Information Security Risk guidance. System 1 is also developing the DOE-IN Certification and Accreditation Transformation Transition Strategy Plan, which identifies the framework and milestones that are being used to migrate to the new standard. System 1 is also providing guidance internally to DOE-IN personnel with respect to the impact of ICD 503 on current operations and the role of continuous monitoring. We have implemented elements of the Site Assist Visit process in the IN environment.

Department of Energy, Office of the Chief Information Officer, Energy Information Technology Support

This contract is to implement a cybersecurity improvement program for Energy Information Technology Services (EITS), which supports DOE Headquarters, program offices (including NNSA), and many of the field sites is well on the way to complete the implementation that incorporates security seamlessly into mission delivery based on risk. This approach implements elements of open government with increased transparency, accountability, and collaboration to encourage EITS community participation. The approach developed by System 1 also



implements organization-wide risk management to reduce costs and to tailor security to the mission.

Ultimately this will lead to cultural change and the incorporation of security through all aspects of the mission and throughout all lifecycle stages. The flexibility of this approach incorporates elements that can be used in the cloud and in mobile devices, and supports the notion of “secure access to information, anywhere, at any time.”

DOE management has approved the approach to build an agile cybersecurity framework, and EITS is currently in the process of implementing many of the measures. Some of these approaches developed and being implemented by System 1 include:

- Risk-based governance –System 1 has issued a revision to the Program Cyber Security Plan and a new governance document (incorporating elements of NIST SP 800-39). These documents realign roles and responsibilities to make decisions more agile and risk based. The approach encourages the mission owners to assess and acknowledge risk in their normal course of business. The new governance process increases the ability to make risk-based decisions while allowing the decentralization of the Authorizing Official from the Office of the Chief Information Officer to the program and staff offices.
- Streamlined processes – The approach has resulted in a number of streamlined processes and approaches. The current process of authorizing systems every three years will be replaced by an authorize once and continuously monitor approach.
- Common Controls that are updated dynamically – A set of common controls (called baseline controls in DOE nomenclature) have been established and are being stored in an electronic repository. This allow the inherence of controls with testing reducing the overhead burden of security.
- Consolidated and simplified cyber architectures – There are approximately 120 systems within EITS. The new cyber architecture leverages concepts in NIST to allow the construction of “system of systems” or enclaves in DOE. This reduces complexity and cost because new systems or tools may be “dropped” into enclaves with predefined sets of controls.
- Risk Tolerance – The degree of security implementation is predicated on executive risk or risk tolerance (the degree of risk an organization will accept). At DOE this is the responsibility of senior departmental management. EITS has identified a method of assessing, measuring, and expressing organizational risk tolerance.
- Continuous Monitoring – The key to maintaining enclave and system authorization is continuous monitoring. DOE is in the process of implementing the elements of a program stemming from NIST (NIST SP 800-137). EITS is implementing a dynamic model to identify



new threats, assess their impact, and implement changes to controls/protective measures to mitigate their effects on a near real-time basis.

System 1 is using these tasks to lay the ground work for implementing a risk based cybersecurity program socializing the architecture with the EITS community, developing training on the “how to” documents initiating the transition process, and changing the culture to ensure the implementation of effective cybersecurity. This effort consolidated headquarters systems into enclaves and significantly reduces the cost of security implementation. These efforts will result in the development of a private cloud for the OCIO developed by System 1.

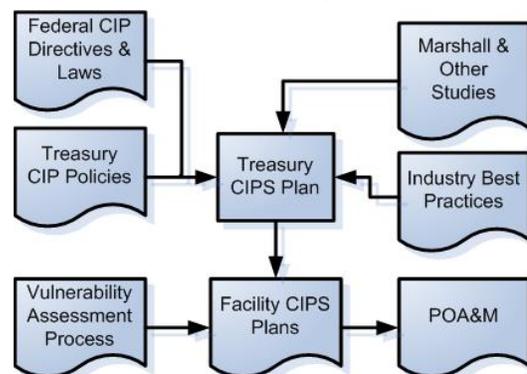
System 1 also supporting NNSA efforts to build and deploy a private cloud with 2NV and YourCloud. We are participating in the cybersecurity Integrated Project Team. The private cloud that we are building for EITS and OCIO headquarters systems will ultimately be housed in the NNSA cloud. System 1 is supporting making these clouds FedRAMP ready as members of the SRA teams, which were approved by FedRAMP and a third party assessor.

Department of the Treasury – Facility Security Assessment Process (FSAP)

System 1 has developed and implemented an approach to evaluating industrial control security to provide input into a unified risk model. This approach has been, and is being used, at the Department of Treasury, and elements of this approach have been used to assess computer security for control systems for large multi-billion dollar physics experiments.

System 1 supported the Department of the Treasury in the development and implementation of a physical and cyber critical infrastructure protection (CIP) program. We have identified the Department of Treasury’s national critical cyber and physical assets and functions.

System 1 has also developed a security convergence solution that is being used at the Department of the Treasury. This was based on elements of NIST SP 800-82, *Guide to Industrial Control Systems (ICS) Security*, NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*, and FEMA Publication 452, *Risk Assessment, a How-To Guide to Mitigate Potential Terrorist Attacks Against Buildings*. The approach resulted in an assessment methodology and framework by which risks from controls systems, physical security, and cyber security could be weighed for Federal buildings. This extended some of the legacy work done by DHS which was terrorist-based to an all hazard approach. It also provided a modular approach with a process template customizable on a per-facility basis. The System 1 approach can be used to establish a balanced picture of the state of security (risks, vulnerabilities, and improvements) so that resources can be optimally allocated.





The approach has been used in the Department of Treasury and is now a standard. The approach is unclassified but the results from its implementation have been classified. This solution provides an integrated view of security:

- Evaluation of existing and emerging requirements to ensure consistency with national requirements/guidance and incorporation of successful security practices and technologies.
- Establishment and implementation of a standard Treasury-wide physical security assessment capability to support the goal of facility certification.
- Development of standardized security processes and artifacts that provide similar roles in both the cyber and physical security communities.
- Support improvements to real-time and ongoing communications to provide warning of threats and to standardize the lines of communications over multiple channels.
- Establishment of an effective security program through improved internal and external communications channels.
- Implementation of a corporate culture of continuous improvement through standardization of security processes and measurement of performance with meaningful metrics.

Department of Energy, Office of Science – Site Assist Visit Process

System 1 developed the Site Assist Visit (SAV) process. The SAV methodology is a comprehensive approach to achieving approval to operate under proper Authorizing Official authorization through understanding risks, confidence in the A&A process, and status of implemented controls. This methodology is an intensive IT business process that integrates information assurance with operational practices, system development life cycle, project management, budgeting formulation and execution, strategic planning, enterprise architecture, and management decision making. The key aspect of the SAV methodology is that it faithfully follows the NIST assessment and authorization risk management framework.

The SAV methodology breaks the usual audit patchwork cycle of fixing problem symptoms, and replaces it by identifying and resolving root causes of problems. The SAV methodology developed is focused on a risk-based, cost effective structure for information assurance through a series of activities that culminate in a NIST and FISMA-compliant certification and accreditation of an information system. Government agencies often struggle with correcting IG or other external audit findings for their information security program. These findings are often stated as “material weaknesses” of the program that require remediation. Often the agency is given a timeframe to accomplish corrective actions. The Agency diligently tries to correct these issues through a “patchwork of solutions” that usually prove to be ineffective in the long run, because while the finding is addressed, the root cause is not. During subsequent audits, the unresolved root cause will result in different “material weaknesses” being identified. The result is that a cyclic process evolves, of identify – fix – identify – fix – etc. The organization fixes what the auditor specifically identifies and not the root causes.



The SAV process brings in other integrated elements of good information management and security, such as the architecture, budget and resources. This results in aligning the responsibilities of mission, support, and security personnel with their respective security roles. There are three phases to an SAV: the discovery phase; the mitigation phase; and implementation phase.

The SAV process builds security artifacts, developed by the client IT staff with System 1 supervision, that provides valuable hands-on experience that is necessary to develop and maintain a strong security program. System 1 works with the local IT staff, following the NIST methodology to:

- Identify threats and risks to information and information systems
- Define and categorize information systems in the current IT environment
- Provide education on NIST information security requirements and implications to the current IT environment
- Conduct a gap analysis and develop a report
- Determine appropriate management, operational, and technical controls
- Develop a Plan of Action and Milestones to implement security controls
- Develop security certification documentation

System 1 personnel also determine how security procedures are integrated into other IT processes, including: strategic planning, system development life cycle (SDLC), project management, enterprise architecture, budgeting, capital planning and investment control, change control, and training.

System 1 has also supported the evolving science cybersecurity research needs across the complex, and has attended and presented key note programs at a number of cyber security research meetings over the last several years. These have taken place mostly in Washington, DC and in Oak Ridge, TN.