

Inspections, Surveys and Self-Assessments

Inspections, surveys and self-assessments are vital to an organization. PNNL's staff are highly regarded for their development of assessment tools that aid in the evaluation of safeguards and security programs. Our staff provide broad expertise in developing inspection tools, evaluating safeguards and security programs, providing concise analysis of the results as well as the ability to develop, implement and teach the assessment and inspection techniques.

Organizations must monitor the performance of their protection programs and perceived strengths and weaknesses. In this area, we cover the spectrum from developing courses and tools to conducting security and self-assessments to corrective action plans and especially root cause analysis. Our staff frequently use the root-cause analysis approach to identify a problem, then trace it to causes such as training, management or human error.

PNNL researchers have discovered that these capabilities not only aid in identifying potential or actual security weaknesses, but also allow us to develop and create new techniques, technologies and capabilities that can better predict, assess and resolve situations before they become a problem.

Technology Development and Deployment

The area of **technology development and deployment** is one of the Laboratory's focal points and an area where great successes are being achieved. PNNL's technical staff identify, test, perform pilot demonstrations and facilitate site utilization of technologies that are currently deployable and will significantly enhance the robustness of the safeguards and security system. Specifically, staff develop and search for high-impact technologies that can enhance our ability to protect critical national assets while reducing operational risks and recurring cost through effective technology deployment.



PNNL engineers have developed miniature radio frequency tags that are ideal for rapid, remote inventory tracking and for monitoring a wide variety of items. We have applied this technology to inventorying sensitive electronic media, tracking high-value military equipment and monitoring environmental conditions of military components.

The Path Forward

The constant evolution of capabilities provides a path forward for growth in field intelligence, counterintelligence, cyber security, infrastructure protection and special operations, to name a few.

Given the competition-based information environment, competitive intelligence is an activity of increasing importance. Whether the need is for knowledge of an industry, a market, a product or a competitor, reliable global information is central to national success. PNNL uses the same techniques and tools for industry and government clients to help them maintain their competitive advantage.

About Pacific Northwest National Laboratory

Pacific Northwest National Laboratory is a Department of Energy (DOE) Office of Science research facility that delivers breakthroughs in the areas of environment, energy, health, fundamental science and national security. Battelle, based in Columbus, Ohio, has operated PNNL since 1965. A unique agreement with the DOE enables us to work with industrial clients and leverage DOE's vast resources. We have a long history of working with industry. PNNL is located in Richland, Washington, and in 2005 had an annual business volume of more than \$700 million and more than 4,000 employees. Addition web resources are at: <http://www.pnl.gov>

For more information, contact:

Michael Schwartz
Information Protection and Analysis Group
Pacific Northwest National Laboratory
PO Box 999, K8-58
Richland, WA 99352
Phone: 509.375.2618
Fax: 509.372.4830
Michael.Schwartz@pnl.gov

PNNL-SA-49763



Pacific Northwest National Laboratory
Operated by Battelle for the U.S. Department of Energy

Information Protection and Analysis



The Value of Protection

The Pacific Northwest National Laboratory (PNNL) Information Protection and Analysis Group (IPSA) offers a wide range of capabilities to help organizations safeguard their information and expand their business practices. Through its highly experienced and specialized technical staff, PNNL consistently strives to develop better tools to identify, track and protect critical information contained within the physical, cyber and human domains. We are assisting both industrial and government clients in monitoring and improving their systems and security posture.

Applying Our Capabilities

Developing a faster way of identifying and addressing incidents that have the potential to develop into security threats is a driving force for PNNL's IPA group. Failing to take the necessary steps to protect information could negatively impact national security, proprietary assets and increase risks. PNNL provides its clients with leading-edge support through its capabilities in:

- Security program development and training
- Workforce analysis
- Technology development and deployment
- Root-cause analysis
- Security program identification
- Site infrastructure evaluations
- Inspections, surveys and self-assessments
- Risk assessments
- Policy development.

The U.S. Department of Energy (DOE) has selected PNNL as a primary resource for conducting security assessment and surveys and also analyzing the results of these evaluations. PNNL has created a 'tool-kit' for the DOE complex that is comprised of security necessities such as policies, procedures, performance tests and evaluation tools that organizations can use to conduct their own security evaluations.



PNNL's Enhanced Security Through Human Error Reduction/Causal Analysis Resources & Tools (ESTHER/CART) program heightens awareness of factors that contribute to

human errors in security incidents and provides resources and tools to improve reporting. This web-based program provides training, job aids and practice in identifying organizational/situational, personal or environmental causal factors. The expected impact will be enhanced security incident reports that better reflect the foundation and appropriateness of corrective actions and, in the long run, a reduction in the number of recurring incidents.



Secure Safe provides a positive technology-based mitigation to combat threats to classified information. This security device sounds an alarm if a staff member leaves the room and specific materials are either not stored in their appropriate location or the container is not properly secured. The system has been deployed at several DOE sites and with

the Defense Department. It has potential industrial applications such as securing bank vaults, hospital medicine cabinets and corporate filing cabinets.

Leaders in the Industry

PNNL's multi-disciplinary team provides a high degree of expertise and knowledge for developing security programs. PNNL staff's diverse expertise includes:

- Counter and antiterrorism
- Analytical experience
- Intelligence and counterintelligence
- Investigations and forensics
- Technology development, application and engineering
- Extensive military experience
- Cyber security, and
- Programmatic evaluation and assessments.

Our staff's close affiliations with the American Polygraph Association, American Society of Industrial Security, Institute of Nuclear Material Management and American Academy of Forensic Sciences help foster collaborative working relationships within government, industry and academia. Our expert staff are key players in the fields of:

- Personnel security
- Operations security
- Communication security
- Information security
- Cyber security
- Physical security
- Information assurance
- Program management
- Technical communications
- Protective force
- Technical surveillance
- Policy analysis and development
- Counterintelligence.

Security Program Development and Training

The **security program development and training** capability at PNNL is focused on the full range of security policies and procedures. Using rigorous security training methodologies, PNNL staff help clients develop and implement security programs.

Training capabilities include the development of computer-based training modules, mobile training teams, correspondence courses, user tools and handbooks as well as the development and presentation of course curriculum.

These capabilities provide internal and external assessment tools in the evaluation of security programs and systems; identification and development of cost-efficient and effective security solutions; guiding the conduct of the security training; and development of security tools to protect the nation's infrastructure.

Again, using accredited third-party administrators, PNNL is able to measure the effectiveness of security training and continually monitor and improve the efficiency and effectiveness of all business practices.

Information Security

Information security encompasses the specific programs, technologies and capabilities that provide expert technical assistance on critical national security matters. Most notably at PNNL is the Information Security Resource Capability (ISRC), which has served as a center of excellence for more than a decade. The ISRC is able to identify and apply technologies to mitigate security threats and vulnerabilities. The ISRC also provides assistance in policy development and implementation.



The PNNL-developed Mozart software can be used by private industry or government agencies as a defensive tool in assessing their websites and to expose unknown targeting, customer behavior activities or even leaks of sensitive information. Mozart incorporates a powerful link analysis and web page prioritization algorithm that enables users to readily find web pages that contain sensitive information.



The Incident Tracking and Analysis Capability (ITAC) was established in 2000 to support the needs of coordinating, analyzing and archiving incidents of security concern. These incidents, at the time of occurrence, have yet to be determined to be a violation of law, but are of such concern to the DOE Safeguards and Security program as to warrant immediate reporting, inquiry, review and subsequent assessment.



Differentiating between classified and sensitive unclassified information is a key issue that PNNL's specially trained analysts manage everyday. The Laboratory has stringent requirements and standards in protecting classified and unclassified controlled information and has adhered to this same level of excellence in supporting clients.

Consistently differentiating between classified and unclassified controlled information is key to ensuring that the proper level of protection is applied. PNNL's specially trained analysts contribute to the development of policies, procedures and other tools that ensure a robust yet cost-effective security program. After the information has been categorized, identified and labeled, specific security measures are incorporated to ensure the information is protected.

Counterintelligence

PNNL is continually looking for ways to improve the processes for information protection through **counterintelligence** activities. These activities mitigate the threat posed by organizations or individuals engaged in espionage or sabotage and are a crucial way to keep awareness at its peak for what could be construed as a potential security threat. To anticipate the next generation of counterintelligence information tools, the need to integrate information from several sources as well as be able to interpret the data and make decisions quickly is key.

Personnel Security

PNNL also operates the polygraph program for DOE. Staff conduct polygraphs of identified personnel for programmatic reasons as well as to assist in the security evaluation of personnel. Aside from tangible capabilities, PNNL also requires that individuals undergo a personnel screening process if their duties necessitate access to protected information. This process can include reference inquiries, verification of qualifications and criminal records checks.