

COMPUTER SECURITY INCIDENT RESPONSE CAPABILITY

FISMA Compliance



CSC
NORTH AMERICAN
PUBLIC SECTOR

CSC

CSC's Computer Security Incident Response Capability (CSIRC) will enable your organization to take a proactive stance by tracking, correlating and remediating computer security incidents faster, while avoiding unnecessary down-time.

Why Choose CSC?

CSC knows how to partner with federal agencies for success. A true contractor-government partnership is one based on total mission commitment and trust. A fine security example of this true partnership is found in the joint vision and the roadmap to effective security management taken by the Environmental Protection Agency (EPA) and CSC. Working in true partnership, our CSC/EPA team improved EPA's historical (D-) FISMA score in 2002 to an A+ in FY2005.

CSIRC Demonstration

CSC's Enterprise Network Managed Services Center of Excellence (ENMS COE) serves as an optimal environment for research, development, evaluation and testing. Automated CSIRC tools are fully available in the COE for demonstration. These tools have enabled CSC to create a standardized, repeatable process, which is cost-efficient to our customers.

IT Infrastructure Solutions

**15000 Conference
Center Drive
Chantilly, Virginia 20151
1.703.818.4300
www.csc.com/itis**

Overview

Even with a strong working security operations center, integrated workflow processes and a certified, trained staff, security architectures can still be exposed to risks. Therefore, you need a comprehensive security management program. Security management in the federal agency domain starts with a sound security policy and ends with automated compliance reports that map back to the management, operational, and technical controls outlined in NIST 800-53.

CSC developed a computer security incident response capability based on a coordinated enterprise-wide approach to security operations, the handling and management of computer security incidents, and security policy. With a security architecture that centralizes security services and security management, our CSIRC is easy to follow, repeatable, scalable and adaptable to pilot program certification.

Features of CSIRC

- Alert notification and reporting
- Patch and vulnerability management
- Incident correlations, resolution and response
- Trend monitoring and logging
- FISMA reports to management
- Certified security professionals

Benefits

- CSC leverages world-class tools to analyze and detect potential and real vulnerabilities on your network. We provide real time alert notification systems when incidents occur. Our integrated solutions are configured with checks and balances.
- Customized access control systems are available for deployment for the highest sensitivity networks. Policy compliance managed systems are setup to allow or deny all data movement to help ensure government regulations are met.
- Our patch management systems are fielded to ensure that all systems are up-to-date against the latest threats. New patches fit into our process in a timely fashion.
- Correlation systems frame small events to create a picture of larger incidents. When events become potential issues, the correlation system integrated into your helpdesk software is used to elevate the importance of negative events. Security professionals are able to work on the highest priority issues first when our best-of-breed tools are implemented. Events become potential issues; the correlation system integrated into your helpdesk software is used to elevate the importance of negative events. As a result, security professionals are able to work on the highest priority issues first when our best-of-breed tools are implemented.
- If your organization follows a standard policy such as FISMA or Sarbanes-Oxley, we generate reports and create task priorities that align with your standard and its categories. Incident response, system standards and your operational procedures align when you use the Computer Incident Response Capability.
- Compliance with NIST 800-53 IR 1-7