Critical Infrastructure Protection and Information Assurance

Synectics has delivered complex critical infrastructure protection (CIP) and information assurance (IA) solutions by deploying emerging technologies and acting as the transformation agent for IT policy modifications that enable these technologies and approaches to operate efficiently and securely in the Enterprise.

Synectics has designed and operated IT security programs and systems as an integral element of our service offerings for HHS agencies for more than 30 years. Mission-critical systems under our care as well as systems that manage billions of dollars annually in federal funds and are used by thousands of users have never experienced any significant loss or disruption.

These include systems that manage sensitive, personally identifiable information (PII), support federal financial management, and manage information that is covered by HIPAA—generally, a broad range of systems that fall within the FISMA low to moderate impact categories. Systems that we have designed and operate are routinely subject to independent, third-party security reviews and audits, including systems that support HHS Health IT investments. In some circumstances, our senior staff personally certifies that appropriate security controls are in place and maintained properly, under risk of personal civil or criminal liability. We approach infrastructure protection and IA with thoroughness and resolute commitment.

Synectics provides a full range of infrastructure protection and IA services. We employ technical staff with appropriate experience, training, and certifications such as Certified Information Systems Security Professionals. We maintain an extensive network of subject-matter experts, independent consultants, subcontractors, and other partners that we draw on as needed for special requirements.

The table below cites our Task Area 7 CIP & IA capabilities under our CIO-SP3 SB contract.

Requirement	Experience and Qualifications
Cyber Security	Deploy a multi-layer, defense-in-depth security architecture and a comprehensive security event management service via a security information management system. These tie into the overarching Enterprise Management System (EMS) providing a holistic view of the confidentiality, integrity, and availability of the monitored environment. Implement a common security infrastructure across all layers and domains to ensure only authorized and authenticated users gain access to critical information in compliance with FISMA.
Critical Infrastructure Asset Identification and Configuration Management Databases	Enforce layered components and centralized monitoring and management. Research new IA software and hardware as technology and requirements change, and add/update/maintain inventory of all IA software and hardware components. Review all Configuration Change Requests (CCRs) to ensure IA compliance. This practice ensures application of best practices for security protection against known and unknown threats.
Information Assurance of Critical Infrastructure	Our security specialists combine design experience for IA of critical infrastructures with the latest developments in information and network security to develop individualized network security solutions for prevention, detection, incidence response, monitoring, and logging network activity. These activities provide improved analysis and definition of security requirements for Multilevel Security (MLS) issues.

Requirement	Experience and Qualifications
Risk Management (Vulnerability Assessment and Threat Identification)	Have expertise in the identification of threats and the implementation of controls to reduce the impact of risks and the ability to document the risks associated with an information system. Complete vulnerability assessments and scans to identify threat identification at regular intervals in accordance with policies and take the appropriate steps to report, remediate, and review system vulnerabilities. Maintain historical records of all scans and perform a system report upon the completion of each test. Ensure all databases are updated with the latest scan information and issue a temporary approval or certification based on the successful remediation or non-event report from the system.
Facility Protection Planning	Provide support for the management, inspection, planning, and execution of significant facility moves. Support facility quality control, physical plant suitability, security, end user devices, VTC equipment, telephony and circuits, as well as overall project planning and scheduling. Our facility protection planning ensures continuous and uninterrupted continuity of service.
Information Systems Security	Ensure the confidentiality, integrity, and availability of our IT systems. Capable in the areas of information systems security, network security, and security analysis. Conduct in-depth technical reviews and validation of all new and existing IT systems to identify potential security problem areas before they arise.
Security Operations Center Development and Operations Mgt	Provide a variety of security operations center development and operations services: security policies, procedures, and guidance requirements, analysis, and modeling; firewall design, implementation, and management; and infrastructure design and security training.
Application Security	Develop defense-in-depth security architecture for protection against cyber threats using content and application security solutions. Invoke levels of testing to determine whether the application is vulnerable to common or unique attacks (such as attacks on application logic). Use penetration testing to simulate the types of attacks, including those that attempt to subvert the application's unique security mechanisms.
Disaster Recovery	Provide support in preparing IT contingency and disaster recovery plans in accordance with federal guidance and NIST Special Publication 800-34, *IT Contingency Planning Guide for Information Technology Systems*. Create contingency and disaster recovery plans and conduct testing on a regular basis.
Critical Infrastructure Continuity and Contingency Planning	Experienced in helping agencies assess incident detection capabilities by identifying and assessing the incident capabilities. Adhere to operational standards for storage and data management, provide personnel skilled in backup and restore activities, monitor server and storage performance including capacity assessment, and conduct performance tuning. Provide COOP environments for application, database, Web portal, and system management/monitoring. Operations and performance schedules are monitored 24/7 in accordance with written protocols.
Incident Response Planning and Execution	Initiate, coordinate, and validate change activities providing the experience to quickly transition when a threat occurs. Detect and remediate application vulnerabilities. Develop, evaluate, and annually test contingency plans to prepare for emergency response, backup operations, and disaster recovery.
Security Certification and Accreditation	Support clients in the development and process of certification and accreditation packages. Provide training to our staff to support federal government agencies by meeting FISMA, DIACAP, and NIST standards and requirements.

Requirement	Experience and Qualifications
Training and Awareness Programs	Training capabilities consist of application support, operational training, and support for major IT systems, training for new applications, infrastructure (database and network administration as well as IT security), Web content, QA, and independent testing.
Exercises and Simulation	Conduct exercises and simulations, prototype analysis, and system operational testing for every differing requirement or integration scenarios. Analyze test results for matches against simulation model predictions. Configure contract hosting servers to support integration, penetration, and runtime error-detection testing, acceptance, production, and Continuity-of-Operations (COOP).
FISMA Implementation Support	Follow the security auditing standards of FISMA, C&A, POA&M, and ATO documents and Privacy Impact Assessments (PIA). Produce and maintain compliant IT security plans.
HIPAA Implementation Support	Offer end-to-end enterprise security architecture with defense-in-depth to provide confidentiality, integrity, and availability of information and to prevent access by unauthorized and unauthenticated users across all layers. Compliance with HIPAA, NIST, FISMA, FIPS, Corporate CIO-SP3, and Government laws and regulations.
Record Management	Develop and review various directives, polices, electronic records management systems, and network security programming including software testing procedures prior to deployments. Provide incident response, reporting, and tracking, along with other computer security support.
Public Key Infrastructure	Monitor customer networks for intrusions and anomalies by using identification and authentication tools, such as PINs, passwords, public key infrastructure (PKI) certificates, and biometrics mechanics; firewalls and routers; malicious code and virus detectors; and intrusion detection and response tools.
Trusted Internet Connections implementation	Maintain and implement a defense-in-depth protection strategy encompassing VPN and PKI-encrypted connections to provide our customers and partners with secure access to data and systems.
Intelligent, Automated Data Collection and Analysis	Created a secure infrastructure that supports real-time data submission from grantees and subsequent processing for over 15,000 submissions. All forms for over 75 socially responsible programs received prior approval from OMB. Users securely submit information through the Web-based system and can print associated reports whenever needed. Our secure sign in system provides identity management and authentication for over 6,000 active users accessing multiple computer application systems.