

Information Assurance

Information Assurance: The Process by which you ensure the confidentiality, integrity, availability and accountability of your information and information systems.

Assessment and Compliance Services

- Certification and Accreditation (C&A) using NIST 800-37, DITSCAP, NIACAP
 - Automated tools to produce and manage C&A packages
- Risk Assessment using NIST 800-30, 800-18 and 800-53 (FIPS 200)
- Vulnerability Assessment / Penetration Testing / IV&V
- Compliance Consulting for: FISMA, Sarbanes-Oxley, HIPAA, Privacy Act

Strategic Services

- Design / Review of technical, managerial and operational policies and procedures
- Disaster Recovery / COOP / Contingency Planning

Integration Services

- Vulnerability Intelligence Solutions (PatchAdvisor)
- Firewalls / VPN / IDS / PKI / Smart Cards / Biometrics

Security Awareness and Training Services

- Web-based and Computer-based (CBT) training programs
- Training Classes for all levels - System Admin to End Users

Program Management Office (PMO) Support

- Program Management and Administrative Support
- Project Management Professional (PMP) Certified Project Managers

Network & Systems Engineering

- Security Architecture Design and Review



Quick Facts

- Founded in 1994
- Small Business
- 2007 revenues of \$37 million
- 200+ staff members
- ISO 9001:2000 certified

Contract Vehicles

- Department of Homeland Security EAGLE
- Department of State HITSS
- Department of State SASI
- Department of Transportation ITOP
- District of Columbia Information Technology (IT) Supply Schedule
- FAA FLITES
- GSA 8(a) STARS (GS-06F-0147Z)
- GSA Alliant (GS-00Q08BND0028)
- GSA IT Schedule 70 (GS-35F-0333J)
- National Institutes of Health CIO-SP2

Contact:

Peter Rath
 Information Assurance Program
 Director, ext. 223
peter.rath@onpointcorp.com

1515 N. Courthouse Road
 Suite 310
 Arlington, VA 22201

703.841.5500 tel
 703.841.5501 fax

www.onpointcorp.com



Representative Experience

National Institutes of Health, Office of Research Services (NIH/ORS)



For the NIH/ORS, OnPoint has provided Information Assurance (IA) services through two different contracts. The first contract is a \$1.5M project consisting of 12 full and part-time individuals working together to provide a variety of IA services to the NIH/ORS ISSO including:

- Development of a Information Security Program compliant with FISMA, HHS and NIH policies and mandates
- Creation of an Information Assurance Program Management Office (PMO), which allowed for centralized management and coordination of IA activities
- Certification and Accreditation (C&A) package development following NIST SP 800-37 and NIST SP 800-18
- Integration and development of an automated C&A tool to assist in C&A
- Ongoing C&A follow-up, including POAM and ST&E completion
- Enterprise Risk and Vulnerability Assessments following NIST SP 800-30
- Producing Disaster Recovery, Contingency and Continuity of Operation and Configuration Management and System Security Plans
- Technical support in the implementation and configuration of firewalls, intrusion detection / prevention systems (IDS/IPS), and application hardening
- Provide basic training to system administrators on integrating security into the life-cycle (development to integration)

During the second contract with NIH/ORS, OnPoint designed and developed an Enterprise Security Policy Architecture. Based on the results of our Risk and Vulnerability Assessments, and experience with the client and industry, we identified the need to create nearly 20 Information Security Policies to provide better security. The policies created by OnPoint's IA Team included:

- IT Security Policy Architecture
- Network Enclave Architecture
- Network User Administration and Permitted Use Policy
- Remote Access and Password Policies
- Configuration Management Policy
- Certification and Accreditation Policy
- Network Assessment and Compliance Checking Policy
- Incident Reporting and Response Policy and Procedures
- Disaster Recovery Policy and Procedures

United States Department of Agriculture, Chief Information Office (USDA/CIO)



For the USDA, OnPoint is providing Independent Verification and Validation (IV&V) services to the Chief Information Office, Chief Information Systems Security Officer (CISSO). On this 5-year, \$1.8M contract, OnPoint has conducted IV&V of nearly 250 Certification and Accreditation (C&A) packages, providing recommendations to the CISSO on needed areas of improvement. Additionally, OnPoint has reviewed the USDA Security Policy Architecture and individual security policies, providing high-level recommendations for improvement.

United States Census Bureau, Chief Information Office (Census, CIO)

U.S. Census Bureau

For the Census Bureau, OnPoint is conducting an Enterprise Vulnerability Assessment of the entire Census network for the CISSO. Spanning over 18,000 IP Addresses and located across the country, The Census Bureau serves as the leading source of quality data about the nation's people and economy – with a high focus on privacy and confidentiality of data. The results of our Vulnerability Assessment will assist Census in FISMA compliance and will provide a roadmap to improve their Information Security Program.

United States Department of Transportation, Federal Railroad Administration (DOT FRA)

In support of the Department of Transportation, Federal Railroad Administration (DOT/FRA) OnPoint provides full Information Security Program support, including technical, analytical, documentation, and tool support for the agency's IT Security and Data Privacy Program.



U.S. Department of Transportation
Federal Railroad Administration

OnPoint produces complete certification and accreditation (C&A) documentation packages for FRA's IT systems (which range in security category and size/complexity). We provide IT security incident response, resolving and reporting on a variety of IT security incidents. This includes coordinating incident investigation and resolution activities with the FRA Information Systems Security Officer (ISSO), Deputy ISSO and the FAA Cyber Security Management Center (CSMC) when an incident occurs. Additionally, OnPoint prepares IT security reports, briefings, attends meetings and provides data call responses. OnPoint updates the FRA IT Security Plan; maintains data in DOT's Enterprise Security Portal and is currently training on CSAM, the new DOT tool for C&A systems; supports annual security awareness training, and conducts Privacy Impact Analysis (PIA) and data privacy reporting as needed.

OnPoint's support ensures FRA's compliance with the Federal Information Security Management Act (FISMA), National Institute of Standards and Technology (NIST) guidelines and Federal Information Processing Standards (FIPS) and DOT Cyber Security Policies