NFF
Delivering Net Results

Information Security 2.0

NFF is a Cisco Gold Partner and is certified as an Authorized Technology Provider for the Cisco Identity Services Engine (ISE) technology. NFF also holds Cisco's Security Advanced Specialization with Gold IronPort Certification.

The NFF team has a long and successful history of providing enterprise security solutions for our Federal, enterprise, and commercial clients. We have evolved our security solutions to meet the challenges of virtualization, cloud computing, and mobility.

Organizations feel the need to support employee "bring-your-own-device" (BYOD) to work policies and desire more secure access for their data center and virtualized resources. Cisco's Identity Services Engine (ISE) is the solution of choice to support this. With ISE–a context-aware, identity-based platform–you can reliably enforce compliance, enhance infrastructure security, and streamline service operations. ISE offers the following benefits:

- Security: Secures your network by providing real-time visibility into and control over the users and devices on your network.
- Compliance: Enables effective corporate governance by creating consistent policy across an infrastructure.
- Efficiency: Helps increase IT and network staff productivity by automating traditionally labor-intensive tasks and streamlining service delivery.
- Enablement: Allows IT to support a range of new business initiatives, such as bring your own device (BYOD), through policy-enabled services.

Taking advantage of Cisco's SecureX Architecture, TrustSec, and the Cisco Identity Services Engine (ISE), NFF provides a policy-governed unified access infrastructure ensuring secure access to data, applications and systems with high-performance connectivity for every device. Blending the power of Cisco's intelligent network with context-aware security technologies, we deliver a security solution framework designed to better meet the needs of the mobile and dynamic network, allowing organizations of all sizes to collaborate easily, apply new computing models, and enable their workforce to roam freely. Below are some examples of the Information Security-work we've done for our clients.

U.S. General Services Administration (GSA)

NFF was contracted to procure, design, and implement a new Cisco Virtual Private Network (VPN) infrastructure solution for GSA, at its three VPN production locations: GSA HQ in Washington, DC; Ft. Worth, TX; and Kansas City, MO. GSA's Office of the Chief Information Officer (OCIO) is responsible for supporting more than 10,000 remote VPN users. The new VPN solution implemented by NFF will enable GSA to

meet the increasing demands of their business lines, multi-media collaboration tools, and the "Anytime, Anywhere, Any Device" initiative. This initiative is to ensure that GSA remains a leader in the Federal space for mobility and Telework.

The new state-of-the-art VPN technology will provide better support for the higher degree of telework and mobility that GSA employees desire, while enhancing their ability to enforce device security posture policies and support all the latest mobile platforms with a single architecture.

The new architecture will also optimize their IT operations by: offering enhanced end-user troubleshooting and reporting tools, utilizing a streamlined authentication process, and offer multi-site load balancing and redundancy to maximize availability of remote access services. NFF team will facilitate the migration to the new Cisco VPN platform, and will provide technical support throughout the project.

MITRE Corporation (MITRE)

NFF has been engaged with MITRE for Security Network Design Consulting Services to develop a Cisco Identity Services Engine (ISE) Lab. This project provides a functional testing environment for advanced security options in which multiple designs and scenarios for Cisco ISE can be tested prior to implementation in their nationwide corporate locations.

NFF facilitated multiple Design Workshops to develop the workflow of features with focus on EAP-TLS Authentication on MITRE's wireless networks, Guest Management, BYOD and Mobile Provisioning, Mac Provisioning and Profiling Services. As and end result MITRE will have a functional ISE Lab in which they can demonstrate ISE functionality via network switches, Wireless LAN Controllers, Cisco VPN AnyConnect software endpoints and integration with PKI.

NFF
Delivering Net Results

Protecting Information & Communication

Metropolitan Police Department (DC MPD)

NFF Engineers implemented MPD's secure communication link to the US Secret Service's Multi-Agency Coordination Center (MACC) in Herndon, VA in support of the 55th Presidential Inauguration. These separate data paths were used to transport streaming video feeds from both MPD and from DC Government's Wireless Accelerated Responder Network (WARN), Naval Research Lab (NRL) and Department of Homeland Security (DHS).

MPD and the Secret Service were able to monitor Inaugural activities from the ground with fixed cameras and roving vehicles, and in the air from helicopters provided by the US Capitol and US Park Police. Due to NFF's efforts and technical design, as well as the unique collaboration between the District and Federal government, the 55th Presidential Inauguration took place under the most technologically advanced security umbrella in U.S. Inaugural history.

Washington Metropolitan Transit Authority (WMATA)

NFF has provided a wide array of security services for the Washington Metropolitan Area Transit Authority (WMATA):

- Led the development of WMATA's IT Security Compliance Programs.
- Incorporating security requirements and standards for agency-wide acceptance and distribution, NFF reviewed, updated, and wrote the security policy and instructions.
- NFF's Assessment Survey documented IT business requirements and developed the WMATA IT Security Department Continuity of Operations (COOP) Plan.
- Acted as the WMATA Security Division representative for Disaster Recovery (DR)planning meetings.
- Certification and Accreditation: Evaluated and tracked the Plan of Action and Milestones that resulted in the Security division General Support System C&A.
- Audit Coordination and Response: Internal OIG: Responded to audit requests by the agency Office of the Inspector General internal audit. Guided agency through the annual external audit, met with the auditors, gathered artifacts requested by the auditor, responded to auditor requests and closed out audit findings by acquiring and providing proper evidence to show compliance.
- Developed IT Non-Compliance Reports for systems identified by the Security Division as not meeting agency information security standards.

DC Government

As the acting DCGOV Chief Information Security Officer (CISO), the NFF consultant designed and executed plans for staffing, organizing, and directing the Chief Information Security Officer Organization. Responsible for technical solution design, development, implementation, and enterprise architecture governance of 85 DC agencies, the CISO assesses overarching security requirements as they relate to solution delivery and network operations.

- Reviewed skills, experience, roles, and responsibilities of current security operations and policy development staff.
- Reorganized security operations and governance function.
- Established IT security policy creation priorities to close mission critical policy gaps in network, system, and application security.
- Planned and executed HIPAA security compliance assessments targeting allied government entities.
- Established a policy creation framework leveraging government and industry wide standards frameworks (e.g. FISMA, ISO, and COBIT).
- Refined the organization's policy review board (PRB) charter, created policy governance procedures, and started disciplined security architecture processes.
- Developed IT security program communications strategy targeting key stakeholders and customers of IT services.
- Conducted FISMA compliance analysis of the DCGOV network security architecture and infrastructure.
- Developed a white paper regarding development and implementation of a HIPAA- compliant private cloud computing solution.

U.S. Census Bureau

NFF has been architecting, implementing, and supporting critical enterprise solutions for the U.S. Census Bureau for 10 years, including: Nationwide information security architecture, hands on solutions integration and testing, design and implementation of Web/Email filtering solutions, preparation of disaster recovery plans for network and security devices, IPv6 testing and transition planning.

NFF deployed a full Cisco Identity Services Engine (ISE) solution for all Wireless networks and manages 7 ISE appliances to support wireless users and 10,000 VPN AnyConnect remote users. A large scale ISE solution for all wired networked devices to support additional 30,000 licenses is currently in process.

SureScripts

SureScripts is the nation's largest E-prescription network, specializing in online prescription ordering. NFF implemented Cisco Network Admission Control (NAC) and Wireless LAN Controller systems mitigating SureScripts' virus and malware-based security threats by monitoring security protection on endpoint devices and enforcing security policies. This resulted in fewer virus infections, fewer help desk calls, and a more resilient secure network infrastructure.