

Why Network Designs

NDI provides IT solutions to customers' unique IT problems.

NDI provides the FASTEST TURN-AROUND possible on complex IT projects—NDI SUCCEEDS 100% of the time.

NDI implements TESTED and RISK-FREE emerging technologies quickly and effectively to achieve increased productivity and revenue for our customers.

NDI principals provide management oversight to ensure superior, PERSONALIZED customer service.

NDI technical managers are SEASONED and have INSIGHT into the DoD & federal markets.

NDI technical staff not only are industry CERTIFIED, but also have a minimum of 3 years of HANDS-ON EXPERIENCE in the IT industry.

NDI is an EXPERIENCED and RELIABLE IT services provider with 7 years of excellent past performance to prove it.

Network Designs provides networked video surveillance, data and physical security, and computer forensics and training in support of Force Protection Initiatives and homeland security.

A **women-owned** business, Network Designs holds GSA Schedules, a Department of Commerce GWAC COMMITS contract, and multiple BPAs with the Federal Aviation Administration and with NAVFAC for IT services.

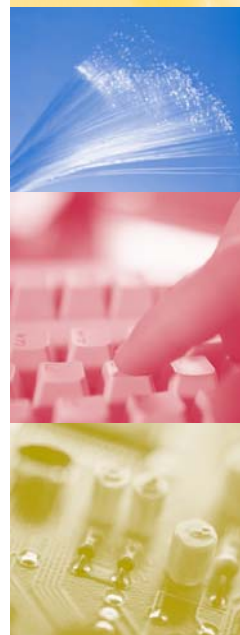
For more information, contact **Nancy Pierce**, Director of Business Development, at 703.268.0030 or visit www.netdes.com.



Network Designs, Inc.
501 Church Street, Suite 210
Vienna, Virginia 22180-4711
703.255.2206 (voice)
703.255.2424 (fax)

www.netdes.com

NETWORK SECURITY



Training Courses on Cyber Terrorism



Network Designs offers on-staff data security professionals with law enforcement backgrounds to provide enterprise network assessment, detection, investigation, prevention, and training.

Cyber Terrorism Investigative Training

In support of Homeland Security initiatives, **Network Designs** offers cyber terrorism investigative training based on decades of hands-on law enforcement and network security experience. Computer crime investigators, experienced in uncovering and documenting fraudulent computer network activity and recovering data loss, apply their knowledge to conduct cyber terrorism trainings at the Department of State, the Department of Defense, the Federal Bureau of Investigation, the National Infrastructure Protection Center, and the Drug Enforcement Administration.

Our Network Security Services Division offers—

- Course Development and Implementation
- Training Nationally and Internationally
- Consulting Nationally and Internationally
- Network and System Support for Courses

Several courses currently in demand include *Cyber Terrorism Executive Seminar*; *Investigating Cyber Terrorism*; and *Protecting Critical Digital Infrastructure*.

Cyber Terrorism Executive Seminar

This seminar is intended for Government and industry executives who direct agency law enforcement operations and other officials who help shape the criminal justice system response to computer-related crime or terrorism.

Network security specialists who set policies and allocate resources to maintain systems security, emergency preparedness, and continuity of operations will also benefit from this course. The seminar reviews the following topics:

- An Overview of Cyber Terrorism
- Terrorist Organizations With Cyber Capabilities
- Critical Infrastructure Targets
- Cyber Terrorism Tactics
- Government Vulnerabilities to Cyber Terrorism
- Historical Review of Cyber Terrorism
- Current Readiness for Cyber Terrorism
- Mock Scenario of Cyber Terrorism
- Identifying the Threat of Cyber Terrorism
- Legal Framework Around Cyber Terrorism
- Worldwide Response to Cyber Terrorism

Investigating Cyber Terrorism

This course is intended for mid-level investigation managers, prosecutors, and support staff involved in the oversight and prosecution of cyber crimes, terrorism, and the seizure of electronic evidence.

The course reviews the following topics:

- A Discussion of Modern Cyber Terrorism
- Motivations and Trends in Cyber Terrorism

- Resources Needed to Build a Cyber Investigative Unit
- How to Seize Digital Evidence
- Media Analysis Process and Tools
- Documenting a Cyber Investigation and Preparing for Court Presentation
- Applying External Resources to Cyber Investigations

Protecting Critical Digital Infrastructure

This course is intended for system administrators and network security specialists who protect network information and infrastructure and investigate and respond to network attacks. The course reviews the following topics:

- Motivations and Trends in Cyber Terrorism
- A Review of Vulnerable Infrastructures
- The Anatomy of a Cyber Attack
- Hardware and software Network Components
- How Routers and Firewalls Work
- Intrusion Detection Systems
- Vulnerability Assessments and Creating a Disaster Recovery Plan
- Gathering Evidence in a Networked Environment

Contact us for further information on course offerings or visit www.netdes.com.

Network Designs, Inc.
501 Church Street, Suite 210
Vienna, Virginia 22180-4711
703.255.2206 (voice)
703.255.2424 (fax)

Contact
Nancy Pierce
npierce@netdes.com
703.268.0030

