

Overview

We turn emerging
technologies into
enterprise
solutions

A Trusted Partner to Customers

Network Designs works hard to earn the trust of our customers. They turn to us because they have unique information technology (IT) problems that require next-generation IT solutions. For our part, we strive continually to turn emerging technologies into enterprise solutions. We envision a ubiquitous access environment, a powerful system of linked networks formed by the convergence of wired and wireless telephony, data, satellite, television, and radio communications. Yet, we are mindful that the convergence of these new network technologies brings technical networking challenges and security requirements to the forefront.

A Seasoned Provider

For over a decade, we have practiced and demonstrated through our past performance how to successfully manage the outcomes of these converging technologies. And over the years, we have honed our technical skills in *network design and integration*; *software applications development*; and *information assurance*. In addition, we have complemented our technical strengths with overall program and contract management for the design and implementation of complex IT projects.

Teamed to Succeed

To provide robust solutions to our customers, we have formed strategic alliances with industry leaders, maintaining certifications, such as, Cisco Premier Partner, Microsoft Certified Partner, Neoteris Partner, Symantec Partner, TANDBERG Premier Partner, and Verint Authorized Integrator. Through our relationships with Cisco Systems, Symantec, and TANDBERG, we offer a broad range of managed services. Through our partnership with Symantec, we provide managed security services via remote security operating centers. And using technologies such as Neoteris and Network IG™, we offer remote or onsite secure network monitoring 24 x 7 to ensure the health of your network.

To deliver tailored solutions to suit our customers' requirements, we offer superior personnel and team with established experts in the IT industry. That's why we assembled a 10-company-strong team of experts to support 11 IT functional areas under the FAA's Broad Information Technology Services II (BITSII) ID/IQ.

We are team members with Northrop Grumman on the R2 ID/IQ contract for CECOM and with General Dynamics on the U.S. Navy Base LAN Information Infrastructure (BLII) OCONUS and Navy Marine Corps Internet contracts. And as a subcontractor to L3-GSI, we support the Nuclear Regulatory Commission, where we manage the network operations center and perform network operational support.



Network Design & Integration

network
operations center
support services

Federal Aviation Administration WJ Hughes Technical Center

Network Designs provided a strategic architecture and design for the FAA WJ Hughes Technical Center. To begin to provide services in this crucial infrastructure area, we collaborated with the customer to identify potential infrastructure deficiencies; define, plan and revise strategies; and then select new technologies to replace or augment existing systems. We followed a design methodology that included risk assessments, needs evaluation, infrastructure design for hardware (voice/data multiplexers, network routers and edge switches), software (voice compression algorithms), evaluation of existing and emerging technologies, site surveys and installation specifications. This project encompassed an in-depth analysis of the Technical Center's network health, including performance assessments, site surveys, requirements analysis, capacity planning, cost and ROI analyses. The completed project concluded with the delivery of a strategic network design and implementation plan. The infrastructure analysis included hardware, software, and protocols. We completed an analysis of several international gateway and message handling protocols and recommended specific protocol implementations.

Federal Supply Service

Network Designs provided network design, network analysis, engineering, installation, operations, and maintenance support for the FSS both nationally and internationally. We conducted desktop management support and operated and maintained the FSS LAN/LABN infrastructure to support the approximately 4000 FSS employees connected to the FSS LAN/LABN. This support—which included premise wiring and cabling, FSS computer room upgrades, and enterprise network/systems management design—was provided to FSS employees located in GSA regional cities, 4 FSS distribution centers, 130 FSS fleet management centers, 11 FSS Customer Supply Centers, 10 FSS remote field offices, 6 sites in Germany, 3 sites in Japan, and in Crystal City, VA.

We monitored over 130 sites and managed the wide area network running with Cisco, Cabletron, and Lucent Switches, routers, hubs, and other telecommunication devices at a centrally located network operation center. The managed network consisted of more than 2000 PCs, some 200 routers, Windows, Novell Netware servers. The full range of supported tasks included managing and monitoring the FSS enterprise network; providing help desk, phone, and onsite troubleshooting for network and system problems; upgrading systems nationally and internationally (operating systems, client software, hardware); providing infrastructure analysis and planning for improvements to the network; providing ISP analysis and services for international sites; providing automated call center support, routing and design; and providing cabling design and infrastructure upgrades throughout the enterprise.

Network Design & Integration

network
operations center
support services

Navy Marine Corps Intranet / General Dynamics and EDS

Network Designs provided inside plant (ISP) and outside plant (OSP) engineering and design to General Dynamics and EDS for the Navy Marine Corps Intranet (NMCI) Program. This project included the evaluation and assessment of existing cable plant (site surveys); recommendation of new cabling requirements and redesign of pathways/conduits; recommendation and installation of switching equipment; customer premise equipment (CPE); and ancillary equipment.

Nuclear Regulatory Commission

Network Designs supports the NRC network operations center (NOC), which is directly responsible for the campus network infrastructure, wide area network (WAN), local area network (LAN), Internet, and remote access at the NRC headquarters and the regional facilities. The NOC provides solution-oriented network services to the NRC using application utilities, monitoring tools, and professional skills. The NOC maintains monitoring systems to ensure service availability and acceptable levels of performance of the network. The NOC supports the NRC datacenter, which houses many critical agency-wide servers and applications and manages a centralized backup system. The NOC supports all WAN connections to the regional office and the Microsoft-, Novell-, and Unix-based servers, as well as the network infrastructure, and the security for the network.

We monitor the network continuously for performance and network load implications. Also, we administer all operational activities on the NRC network equipment including monitoring, managing, maintaining, and troubleshooting for the Access-Layer and Core-Layer Network Infrastructure. We support network wiring, power, and other infrastructure maintenance for the user and core router/switches within the NRC network. We perform network maintenance to the infrastructure to include troubleshooting problems, identifying their cause, and replacing or repairing defective equipment. We create and maintain detailed documentation of the network required for proper network maintenance, operation, and planning. The documentation includes the maintenance of the NRC name space and the assignment of names and network addresses (IP numbers). To ensure smooth network operations, we constantly monitor traffic flow to optimize network usage, to detect network problems, and to ensure equitable access.

Network Design & Integration

network
operations center
support services

US Bureau of Census

Network Designs served as an independent contractor to provide direct technical oversight for the decennial network, DecennialNet. We designed, implemented, and managed a state-of-the-art Network Operations Center (NOC). The NOC we managed was responsible for the overall Census enterprise network. We ensured that the existing Bureau of Census (BOC) network remained operational while a parallel DecennialNet was deployed throughout the US, Alaska, Hawaii, and Puerto Rico. The experience of maintaining operational capability for two networks during a rapid deployment schedule ensured that a transition from the existing network was accomplished in a smooth, orderly fashion. The ATM network was upgraded to a Gig Ethernet Backbone and the connection speed was upgraded to the regional offices connectivity via the Frame Relay Wide Area Network (WAN).

We installed best-of-breed network management systems (NMS)—HP OpenView Network Node Manager, CiscoWorks2000, and Concord Network Health, for fault, configuration, performance, account, and security management of the DecennialNet. The NMS tools were installed on Unix platforms, with full redundancy and failsafe, fail-over operations provided by the implementation of the auxiliary NOC. We implemented pager alert notifications from the NMS for all DecennialNet technical team members. We also implemented a Web-enabled, password-protected portal, CustomerNetSM on the Census Intranet that provided a single point of access to all NOC NMS tools and reports. As the complexity of the DecennialNet increased, network management tools and procedures were enhanced to ensure maximum management control.

We developed, implemented, and validated a comprehensive Disaster Recovery and Contingency Plan for the decennial census. We designed and configured the network routers to reroute all remote Census office connections from any region to the designated backup and recovery facility in the event of the catastrophic loss of a central facility. The complex routing configuration plan required that all remote and central users and servers would communicate via both IP and IPX without interruption. We successfully demonstrated the disaster recover plan in a live test in which an entire region was shut down in a simulated failure and rerouted to the recovery facility. During the disaster test, we coordinated all communications with the Census and the communication providers as well as implemented the router failsafe, fail-over procedures.

Software Applications Development

database
development and
administration

US Department of State Bureau of Diplomatic Security

Network Designs was awarded a \$4 million task order by the U.S. Department of State, Bureau of Diplomatic Security, Office of Antiterrorism Assistance to design and develop a cross-agency Government Information-Sharing Infrastructure (GISI), which comprises both (1) A software application that integrates the latest technologies with the latest intelligence assessments used in the United States by law enforcement agencies to address the methodical pursuance of a case and (2) A networked database system, which can employ either dial-up or satellite network communication.

The GISI networked database system can be retooled and reused by the Department of State in other situations in which a government-wide system of information gathering and sharing is required.

The GISI offers the following benefits:

- Case Management—Software supports all stages in the pursuance of a case.
- Information Sharing Platform—Solution enables the user community to collaborate and share information in a secure environment.
- Process-Driven—Best Practices are used to govern the flow of information.
- End-to-End System—Solution can include computers, networking hardware, and software.
- Sophisticated Data Analysis—Software framework and tools are used to find patterns within large amounts of seemingly unrelated data.
- Language Independent—Software inherently supports multiple languages.

GISI Technologies

Public Key Infrastructure (PKI)—Industry standard providing core security, encryption, and signatures.

Application Server—Apache, Sun Tomcat Web software.

Database Server—Postgre SQL, Red Hat Linux Open Source Platform.

Software Development Tools—Open source. Source code version control using CVS; G-Forge Build Management.

Software
Applications
Development

database
development and
administration

Federal Aviation Administration Office of Rulemaking

Network Designs developed the Integrated Rulemaking Management Information System (IRMIS) for the FAA Office of Rulemaking (ARM). IRMIS is a web-enabled document management system and workflow management application that the FAA designated as one of 22 mission critical business applications. The FAA Chief Information Officer and the Department of Transportation Inspector General praised the IRMIS application as a "best practice" business practice approach to Internet/Intranet-enabling technology that should be implemented and/or duplicated throughout the FAA.

The IRMIS application tracks and reports on the rulemaking life-cycle, including rulemaking schedules, staff, and publication information. IRMIS is a Web-based system accessible via the FAA intranet for the Office of Rulemaking (ARM). IRMIS is fully integrated with CyberDOCS and uses n-tier application architecture; COM+ ; Java Script; Object-Oriented Methodology; Crystal Reports; Java Applets; OLE; XML/XSL. Based on excellent past performance in support of enterprise database applications for the FAA, Network Designs has been awarded additional applications development work throughout the agency.

Federal Highway Administration

Based on the successful design and implementation of the Integrated Rulemaking Management Information System (IRMIS) at the FAA, Network Designs built a Phase I Web-based system for the tracking and management of Federal Highway Administration (FHWA) rulemakings. Implementation of a document management system for FHWA was implemented during Phase II of the project. The work performance on this task included document management; office automation, system administration and user support; information resource management; and systems development.

Software Applications Development

database development and administration

Federal Aviation Administration Office of Aviation Medicine

The FAA Office of Aviation Medicine (AAM) selected Network Designs to develop the Compliance and Enforcement Tracking System (CETS) to track and report on drug and alcohol testing, inspections, investigations, and voluntary disclosures among some 7,200 companies within the aviation community. Currently inspected on a ten-year cycle, the aviation community will be inspected on two-year cycle by employing an increased number of inspectors and by using CETS.

The CETS application was designed to accommodate several conditions: extract and preserve data from the legacy database; pull data from other FAA databases on different platforms; integrate the new CETS application with a COTS-based document management solution; service an inspection workflow comprising inspectors and remote and local users gathering data from 7,200 sites across the United States.

The level of effort required to develop CETS is described below, with details regarding requirements analysis; prototype/system design; application development; installation and testing; system documentation; training on the new system; and final data transfer and deployment of the new system. Already CETS is being used to track and report on the compliance life-cycle, including inspection schedules, staff, and correspondence. The use of CETS has reduced the quarterly scheduling of inspections from a matter of weeks to less than an hour. Inspectors can now enter all enforcement activities data while in the field and upload that information to the FAA server upon return to the office.

Requirement Analysis: Requirements gathering and analysis was a critical step in the CETS software development process. Gaining insight into the existing workflow and the ultimate needs of the end-user provides a blueprint for the final design of a working prototype. Given the nature of the data and the inspection workflow processes that needed to be captured, we very thoroughly reviewed every aspect of the requirement phase.

We analyzed the existing inspection workflow that is currently in use to address the following requirements: Information to be carried over to the new system; Data fields that are no longer necessary; What, if any, existing code can be reused.

Our analysis also included gathering and understanding the following: Web-workflow process; Business rules; Downloadable template requirements; Reporting requirements; Integration requirements; Security requirements; Document management requirements; External FAA system database requirements.

We produced a final requirements document that contained all of the information listed above and a clear road map to produce a database design that meets the needs of end users and fulfills AAM strategic goals.

Software Applications Development

database development and administration

Federal Aviation Administration Office of Aviation Medicine (cont.)

Prototype/System Design: We proposed a 3-Tier Architecture System Application Design that satisfied the requirements of a large-scale intranet/laptop/server application, delivering an enterprise-class application for the FAA AAM. The CETS 3-Tier Architecture provides the physical partitioning of the application:

Graphical User Interface: Provided the client with a seamless interface with the system through the use of fields, drop-down menus, and pre-populated information

Middle Tier: Was implemented as a collection of components that were used in a variety of client-initiated business processes; Provided the ability to call on other components to help implement a request; Provided the method to send client requests using object name to server to obtain information from the database; Provided components to act as gateways with other mainframe databases; Provided the ability to incorporate Custom-Off-the-Shelf (COTS) applications; Provided the ability to add a new component and or new component capabilities without interrupting the client

Server Tier: Provides storage where the database is maintained; Provides added security by not exposing the database schema to the client; Provides added security by ensuring authorized-only access to the server; Provides the ability to update, add to, and delete without interrupting the client

The 3-Tier Architecture allows the FAA CETS System Administration to be less complex. CETS can be centrally managed on the server using standard system management tools. The availability of the application is constant. The tiers can be restarted on another server in case of resident server failure. The end result is a secure, robust system, allowing the application to increase in scale without a complete re-code. The CETS design included the following documentation: integration configuration with other FAA systems; Database structuring/modeling; Integrated security system plan; System objects; Workflow and dataflow; Layout and design of reports; Mock-up, including WEB GUI and application flow; Overall system architecture.

Test Installation, Functional Testing, and Training Documentation: Network Designs produced a series of CETS testing and training documents to ensure that the CETS application met the expectations of the FAA AAM. We produced a comprehensive Test Plan to guide both our developers and FAA users through the application testing process. The process included a uniform testing procedure, the ability to capture the testing results, and the process to be carried out during lab testing and debugging. We documented the procedures to install the CETS application on a server and individual computers to ensure a uniform and successful installation. We performed a full production testing of the CETS Application in a Lab environment. Using the CETS Test Plan, the CETS Application was tested by both CETS end-users and our developers in the real-world environment. Based on the Test Plan, we produced training materials in support of User Training.

Software
Applications
Development

database
development and
administration

Federal Aviation Administration Office of Aviation Medicine (cont.)

CETS System Documentation / Implementation Plan to Production Environment: Network Designs produced all necessary documentation of the CETS system. The documentation included a Data Dictionary (database descriptions), coding script (with comments, i.e. history of changes), source code, test cases, installation script, updated component design and disaster recovery plan. The final document consolidated information from these specified documents along with additional operational and maintenance guidelines in the form of an Operations and Maintenance Plan to be used for on-site maintenance purposes.

We produced the CETS User Manual for end-users to successfully use all aspects of the CETS Application. After the final review of the User and User Training Manuals, we updated both manuals, as necessary, and produced final documents. Our staff traveled to Oklahoma City where the production server is located to perform deployment activities involved in the initial transition of system to production environment. Also, we provided on-site User Training in August 2004 at four sites: Atlanta, GA; Los Angeles, CA; Fort Worth, TX, and FAA Headquarters in Washington, DC.

Final Data Transfer and Deployment of New System: In September 2004, data from the old CETS version (2.0) was successfully migrated into the new version (3.0). After creating and employing a utility to facilitate and ensure a comprehensive and secure transfer of data, we successfully brought CETS 3.0 online as the new Compliance and Enforcement Tracking System.

Software Applications Development

Web solutions

Federal Aviation Administration Office of Public Affairs

Network Designs designed and developed the new FAA Employee Web Site and the new Public Web Site. We reviewed and analyzed the FAA Web Sites using focus group tests, customer surveys, and pilot tests. We then redesigned and retested the sites.

The Employee Web Site consolidates employee information into one area and centralizes Web management for the entire FAA. Read more in the September Issue of the FAA Intercom:
(<http://www.faa.gov/Newsroom/intercom/2004/Sept2004.pdf>)

The Public Web Site (faa.gov) provides logical topic headings and consistent navigation to the general public using the latest technologies.

Methodology Highlights

- The solution provides improved internal and public communications
- Employee-related information is removed from the FAA Public Web Site
- Content is organized by topic instead of by internal organization
- Out-of-date content is deleted
- Content is rewritten using Plain Language principles and Web writing Best Practices

Solution Tasks:

- Project management
- Web design based on expert analysis, and development
- Database registry for all Web sites, developers, and content owners
- Development of official templates
- Web site maintenance
- Content revision and development; training in the use of official templates, Plain Language principles, and writing for the Web

Information Assurance

data and physical
security

Federal Aviation Administration Office of Aviation Safety

Network Designs provides program management and technical support services to the FAA Office of Aviation Safety, Information Technology Branch (AVS-11) Information Systems Security (ISS) program. Since the 1998 release of Presidential Decision Directive 63 (PDD-63)—establishing stringent requirements to protect U.S. critical infrastructure against cyber threats—we have participated in creating new, unique, and FAA-centric information security practices and methodologies at the agency.

Over the years, Network Designs professionals have performed an array of tasks for AVS in the areas of information security management, assessment, and policy formation. Most notably, we developed a risk assessment methodology called the Quick Look Risk Assessment (QLRA), which shortened the time and lowered the cost of completing a full certification and accreditation effort. The FAA Office of Information Security (AIS) later adapted our risk assessment document templates into the FAA's formal risk assessment process.

With the emergence of new Homeland Security Directives, we have evolved our ISS practice to include regulatory compliance and FISMA metrics and reporting.

Overview of Information Security Tasks

- Provided *program management and coordination* with other FAA lines of business.
- Drafted *AVS-specific* policies and plans to implement agency-wide security requirements and *information security policy*.
- Developed a *Rules of System Use* to ensure AVS's compliance with NIST guidance and GAO/IG recommendation.
- Created and documented a conceptual and *technical architecture* for the AVS information security program.
- Performed *risk and vulnerability assessments* for all AVS mission-critical systems.
- Drafted the FAA's initial *Computer Security Incident Response (CSIRC)* concept of operations.
- *Managed information security* software analysis, testing, deployment, and maintenance.
- Performed *asset identification, valuation, and annual loss expectancy* calculations. This responsibility was challenging given the lack of available original asset cost information. To overcome the challenge, our staff developed a formula using commercial prices discounted to reflect FAA's access to volume discounts and calculating loss expectancy based on industry and government surveys and data.

Information Assurance

data and physical security

Federal Aviation Administration Office of Aviation Safety (cont.)

- *Coordinated system criticality assessments* in which we work with system owners and support staff to evaluate the system's requirements for confidentiality, integrity, availability, and accountability.
- *Managed system remediation* and countermeasure implementation. After completing a risk assessment, our staff prepares recommended steps for correction or mitigation of any security risks.
- *Managed Certification and Accreditation* for both critical and non-critical systems. Network Designs prepares all AVS Security Certification and Accreditation Packages (SCAPs) and provides briefing material to support decisions to certify and Designated Approving Authority (DAA) decisions to authorize each system to operate.
- Assisted AVS in "getting to green" on the FAA goal to *Certify and Accredite 100%* of its application systems by the end of fiscal year 2004.
- Coordinated *contingency and disaster recovery planning* both for physical sites and for application systems.
- Carried out *system security testing*. Our staff performs all AVS system tests and evaluations (ST&Es).
- Administered *cost tracking and monitoring*. The Network Designs program manager tracks costs and financial metrics and provides financial tracking for AVS's ISS program. This includes preparing budget projections, documents such as Exhibit 300-Bs and RPDs, as necessary; identifying the source of funds for input to the FAA budget process; and ensuring that budget formulation is coordinated with execution. It also includes tracking obligations and expenditures as they take place using a "checkbook register" approach.
- Supported the effort to incorporate *information security requirements* into the *AVS System Development Life Cycle*.
- Designed the *web page* for the AVS ISS program's intranet web.
- Implemented and maintained a *document management system*, including DM software, to track secure Certification and Accreditation and other sensitive documentation.
- Provided support for AVS input to FAA decisions regarding *enterprise security tools*, such as patch management, scanning, audit log monitoring and review.
- Developed and documented a standard set of AVS Information Security Requirements based on experience with C&A actions and drawing on AVS, FAA, and federal policies and regulations.

Information Assurance

data and physical security

Federal Aviation Administration Office of Aviation Safety (cont.)

Notable Projects

FAA's Information Systems Security Handbook. Network Designs supported the development of the FAA's Information Systems Security Handbook. The Handbook defines the FAA-wide information security requirements and the risk assessment methodology to be used by all FAA organizations. We tailored the risk assessment templates to the FAA AVS environment by adding AVS-specific security requirements. The assessment methodology can be applied to business risks including aviation safety and regulatory compliance. Risk assessments identify assets or business processes that require protection, risk mitigation techniques, or impact analysis or that are exposed to threats or vulnerabilities. We provide recommended risk mitigation strategies and tools. Each of these steps results in a quantifiable metric that compares the overall risk and strength of mitigation to comparable environments at the FAA. Because of Network Designs' depth of knowledge in this area, we are intimately familiar with government and commercial risk analysis methodologies, requirements, and mitigation techniques, including internationally and nationally recognized information security standards such as International Standards Organization (ISO) 17799, NIST 800-xx guidelines, DOT guidance, GAO, and DOT Inspector General (IG) recommendations.

Risk Assessment Process and Documentation. We use automated tools to assist in the risk assessment process and documentation. For our FAA clients, we have prototyped the use of vulnerability scanners (i.e., Foundscan, Cybercop), including front-end software designed to simplify the user interface. The end result of our risk assessment work in AVS was a formal Risk Assessment Report, including recommended alternatives.

Disaster and Contingency Plans. Network Designs has assisted clients at the FAA and other agencies with the development of Disaster and Contingency Plans for business continuity in the event of a disaster or a crisis that disrupts availability of systems. Contingency plans consist primarily of "what if" analyses that examine all potential risk scenarios and then recommend the survival methodology best suited to the enterprise or specific systems. Network Designs prepared a risk assessment and Continuity of Operations Plan for the Overflight Accounts Receivable Management Information System (OARMIS) owned by the FAA's Accounting Operations Division (AFM-215).

Failure Mode Effects and Criticality Analysis. Network Designs performed this analysis for OARMIS as an informal part of contingency planning. We examined all potential problems in design, construction and implementation, business process, safety, and environmental issues.

Information Assurance

data and physical security

US Department of State Bureau of Diplomatic Security

We assist the Department of State, Bureau of Diplomatic Security, Office of Antiterrorism Assistance (DS/ATA) to combat cyber terrorism worldwide through a training program designed for friendly foreign governments to deter and counter threats of terrorism. The training program enables foreign countries to prevent, detect, and investigate cyber terrorism incidents. We also introduce state-of-the-art computer forensics hardware and software techniques to enable countries throughout the world to assess and solve computer-related crimes to protect their citizens from cyber terrorism.

In support of the DS/ATA, we have developed a cyber forensics curriculum; created a mobile training lab; and developed training materials. We implement each of these functions when we train program participants at client locations around the world. Current courses include Cyber Terrorism Executive Seminar; Investigating Cyber Terrorism; and Protecting Critical Digital Infrastructure.

Cyber Terrorism Executive Seminar. This three-day seminar is designed to brief foreign government heads and security chiefs on the various types of cyber crimes and the methods to identify reactive and proactive means to address them.

Investigating Cyber Terrorism. This week-long course consists of a full lab setup and hands-on training for field investigators on how to fully prepare for and investigate cyber crime. It was modeled after the U.S. FBI methods of securing and investigating cyber crime-related cases.

Protecting Critical Digital Infrastructure. This week-long course is designed to train security chiefs in a given country and covers how to protect country- and mission-critical infrastructure components.

We have provided training in Malaysia, Philippines, Greece, and other countries, furnishing training and permanent labs in each of these locations stocked with state-of-the-art security and investigative tools.

We use both commercial- and government-off-the-shelf tools—and UNIX, Linux, Windows, DOS, and other operating systems—in the training lab to duplicate a wide variety of realistic scenarios of cyber crime at each training session. Each lab setup is designed to implement the necessary tools that would be encountered by the client foreign country during the normal course of investigations.

Our deployment of these courses has resulted in positive feedback and additional requests for training specific to unique security situations in foreign countries.

Information Assurance

data and physical security

Department of Transportation Office of the Secretary of Transportation

In compliance with Homeland Security Presidential Directive (HSPD) 12, Network Designs has designed a common architecture that is the foundation for the Common Identification System (CIS) at the Department of Transportation (DOT), Office of the Secretary of Transportation.

The CIS will provide both physical and logical authentication that is responsive to different levels of threat across the DOT enterprise. And the solution will include Public Key Infrastructure (PKI)-based e-Authentication for physical and logical access controls.

System Benefits:

- The CIS will require multiple-factor authentication for physical and logical access to DOT resources.
- Current physical authentication based on photograph identification will be upgraded to the swipe of an access card and entry of PIN and/or biometric information, depending on the level of threat.
- The logical DOT architecture that currently supports authentication by user ID and password will be replaced with authentication by Smartcard-based X.509 certificates using two-factor authentication.

Network Designs, Inc.
501 Church Street, N.E.
Suite 210
Vienna, VA 22180-4711
Phone: (703) 255-2206
Fax: (703) 255-2424

Contacts
General Information
703.255.2206 extension 241

Sales & Solutions
703.268.0030

TANDBERG Support
703-880-5208

