Northrop Grumman Overview
• Company Overview
• Locations & Innovation Centers

Global Security Capabilities
• Critical Infrastructure Protection
• Cybersecurity
• Geospatial Intelligence
• Command, Control, Computers, and Communications (C4)
• Big Data Management and Analysis
• Decision Support
• Systems Integration
• Unmanned Systems
• Training
• Fraud Prevention

Global Security Products
• SecureSite
  - Tailorable Integrated Security Solutions (TISS™)
  - Integrated Base Defense Security System (IBDSS™)
  - ExTASS™
  - Harbor and Coastal Surveillance

• SecureC4
  - Integrated - Joint Operational Command and Control Services (I-JOCCS™)
  - LiNx
  - CommandPoint™
  - Public Safety Broadband Wireless
  - Airport Real-time Collaboration (ARC)

• SecureCyber
  - CyberSecurity Operations Center (CSOC)
  - Cyberspace Solutions Center
  - Advanced Malware Platform (AMP) - Dynamic Email Protection
  - SPIDA™

• SecureEnergy
  - Power Grid Dashboard
  - PowerGrid
  - SPUOS™

• SecureEnvironment
  - Environmental Decision Support System (EDSS™)
  - MOREPower™
  - Energy Decision Integration Platform (EDIP™)

• SecureHealth
  - Enterprise Environmental, Safety & Occupational Health (EESDH)
  - PROMIS
  - Public Health Threat Vectors (PHTV)

• SecureData
  - DataMS™
  - GeoHome
  - AppsEnable™
  - Paradigm
  - Agile Client™
  - RePLACE
Northrop Grumman Corporation

Northrop Grumman offers a portfolio of innovative systems and solutions to meet our customers’ global security needs. Northrop Grumman proudly continues to deliver innovative capabilities and products as we have done for more than 50 years. Our Information Systems, Aerospace Systems, Electronic Systems, and Technical Services sectors use proven technologies to affordably meet exacting applications.

Information Systems

We serve customer needs for advanced information solutions for defense, intelligence, civil, and commercial enterprises. Our key products include cyber security solutions; automated biometric identification systems, health information technology; operational command and control systems; networked communications, intelligence, surveillance, and reconnaissance systems; enterprise systems; advanced networking solutions; unmanned ground systems; 911 public safety systems; and systems integration services.

Aerospace Systems

We partner with customers to deliver manned and unmanned aircraft, space systems, and advanced technologies critical to the nation’s security. Our key products include Global Hawk, Triton, Fire Scout, Firebird, BAT, and UCAS-D unmanned aircraft systems; B-2 bomber; James Webb Space Telescope; E-2 Hawkeye; Advanced EHF communications payload; Joint STARS targeting and battle management system; and Space Tracking and Surveillance System.

Electronic Systems

We supply customers with airborne radar, navigation, electronic countermeasures, airspace management, space payloads, marine and naval systems, communications, bio-defense, and government systems. Key products include active electronically scanned arrays (AESA) payloads for F-16, F-22, and F-35; airborne early warning and control radars; integrated bridge systems; Ground/Air Task Oriented Radar system; LITENING targeting and sensor system; systems for digital electronic warfare, aircraft missile defense and air defense; and situational awareness and fiber-optic gyro-based navigation.

Technical Services

We enable customers’ missions through life cycle solutions and innovative technical support and services globally. Key services include Nevada National Security Site management and operations; U.S. Army Mission Command Training Program; Hunter unmanned aerial system life cycle support; platform sustainment and modernization; advanced training solutions; high technology engineering services; operationally responsive systems for KC-10 Extender refueling aircraft, Intercontinental Ballistic Missile Program, U.S. Army National Training Center, and tactical wheel vehicle fleet management.
Northrop Grumman Corporation

Northrop Grumman has a range of industry-leading capabilities to serve our international customers in 25 countries. Our regional business development offices and local businesses in over 30 locations are ready to serve customers in key international locations in Europe, the Middle East, and Asia Pacific regions.

Northrop Grumman’s Innovation Centers are available to assess the most affordable and effective solutions tailored to meet your global security needs.

Corporate Headquarters:
2980 Fairview Park Drive
Falls Church, VA 22042
703-280-2900

Offices in all 50 US States, Major presence:
- Northern Virginia
- Baltimore Metro Area
- Los Angeles Metro Area
- Colorado Springs
- San Diego

Select Offices Abroad:
- Australia
- Belgium
- France
- Germany
- India
- Italy
- Japan
- Korea
- Saudi Arabia
- Singapore
- Switzerland
- Taiwan
- United Arab Emirates
- United Kingdom

Corporate Centers of Innovation
- Center for Innovative Solutions – McLean, VA, USA
  - Center of Excellence for collaboration on tailored information systems solutions
- CyberSpace Solutions Center – Millersville, MD, USA
  - Adaptable, scalable environment to host network defenders for rapidly establishing cybersecurity solutions
- CyberSecurity Test Range – Farham, United Kingdom
  - Evaluation of threats on large scale networks
- Public Health Research and Demonstration Center (RaDC) – Atlanta, GA, USA
  - Adaptation of rapidly changing technology to public health
Northrop Grumman Global Security

CAPABILITIES

• Critical Infrastructure Protection
• Cybersecurity
• Command, Control, Computers, and Communications (C4)
• Big Data Management & Analysis
• Geospatial Intelligence
• Decision Support
• Healthcare Fraud Prevention
• Unmanned Systems
• Systems Integration
• Training

THE VALUE OF PERFORMANCE.

NORTHROP GRUMMAN
Protecting critical infrastructure is one of the highest priorities for nations, localities, and commercial entities. Leveraging corporate expertise in surveillance, intelligence, and networking technology, Northrop Grumman provides Critical Infrastructure Protection (CIP) from the national level to the site level.

**Demand Description**

Today’s threats demand integrated solutions to make comprehensive assessments and direct rapid responses. In order to ensure the right alerts go to the right people at the right time, CIP managers need a proven combination of information analysis, physical security, and cybersecurity.

**Offering Description**

Northrop Grumman’s CIP solutions process data gathered from multiple sources into actionable intelligence to assure situational awareness support swift, sure decisions. Our domain expertise informs the most effective ways to protect sensitive information while keeping communication channels open for sending actionable information to the right people at the right time.

**Integrating protection across all levels**

From the national level to the site level, our capabilities support integration of terrorist threat vectors. We extract and correlate global intelligence into reliable threat assessments for use by national, state, and local authorities to assure preparedness. Our solutions continue to furnish the best available intelligence, even during actual incidents or disasters. They help guide command and control actions needed to optimize response efforts; and give first responders the critical information they need to take the most effective actions.

**End-to-end solutions based on comprehensive capabilities**

- Physical security
- Information assurance
- Identity management
- Identification & authentication
- Multi-security classification
- Biometric technology
- Smart Cards & other ID cards
- Imagery & geospatial systems
- Automated fingerprint processing
- Security screening
- Knowledge/case management
- Data sharing/exploitation

Our proven combination of information analysis, physical security, and cybersecurity protects critical infrastructure for the defense and intelligence communities, at multiple levels of civilian government, and for our commercial partners.
From leading-edge microelectronics to the largest, most complex system-of-systems in the world, the breadth, depth, and capability of Northrop Grumman’s C4 systems provide the tools necessary to act with speed and confidence.

Demand Description
Key decision makers across an enterprise need common access to critical information. They need all pertinent data to be correlated, with the capacity to track all management activities on geographic displays. The short event time to respond requires effective, reliable decision aids and planning tools.

Offering Description
Northrop Grumman provides net-centric open architecture environments to meet customer’s C4 missions and affordably accommodate new capabilities quickly and with minimal risk. Our domain expertise is built into the design, development, production, integration, and installation of C4 systems.

Superior Communications Availability
First responders need reliable access to communication in a crisis. Northrop Grumman has delivered independent wireless communication capability to customers ranging from emergency responders in New York City to warfighters overseas. Whether the need is persistent and planned or deploys at a moment’s notice, our solutions keep secure communications up and running.

Integrated Command and Control
When decision-makers are on site, Northrop Grumman provides command and control infrastructure to suit their needs. Our rapidly deployable, transportable command centers provide secure communication and computing infrastructure with independent power, air conditioning, and lighting.

Maximizing Computing Resources
By using common IT infrastructure for C4 systems, Northrop Grumman reduces the total ownership cost for our customers by eliminating distinct networks and computing infrastructures. Software development and integration replace multiple standalone information systems with a single software product.

From Data to Actionable Knowledge
With numerous data collections systems providing raw information to human operators, Northrop Grumman recognizes the need to distill large amounts of data to useful knowledge so decision-makers can quickly choose the best-informed response possible. We are incorporating recent advances in neuroinformatics, bioinformatics, and bioengineering into our human factors considerations to reduce the analysts’ cognitive workload and improve the quality of knowledge available.
**Big Data Management and Analysis**

Ingest high volumes of data, perform real-time analytics, and enable human driven interactions

By combining capacity to ingest massive volumes of data with commensurate large-scale storage, coupled with requisite processing speed, Northrop Grumman delivers systems to manage the increasingly unwieldy world of Big Data.

**Demand Description**
Commercial enterprise and federal agencies seek effective management of operations involving multiple sources and volumes of data. Users need powerful tools for continuous monitoring of very large data sets, including metrics, alerts, reports, and dashboards. Drivers for big data management and analysis solutions include:

- Exponentially growing volumes
- Increasing requirements for querying
- Need for efficient access
- Scalable architectures to ingest, process, store, analyze and disseminate
- Ability to match volume, velocity and variety to throughput, completeness, and quality to serve enterprise-wide missions.

**Offering Description**
Northrop Grumman employs proven analytic and visual navigation tools to intelligently combine multiple sources of information. Our domain expertise in managing and exploiting large and distributed data sets includes capabilities to identify trends and clusters, and trigger alarms when established thresholds are exceeded. Our Big Data and Analysis solutions enable cost savings through prediction, detection, and analysis of potential fraud and abuse. Our automated data discovery, information validation methodologies, and highly effective analytics provide mission-oriented outcomes for commercial enterprises and federal agencies.

**Fraud Detection**
Northrop Grumman’s proven methods to detect and prevent fraud provide our customers solutions with:

- Real-time analysis of financial markets for fraud indicators, risk profile and potential impact
- Proactive data mining, fusion and predictive analytics for fraud, waste, and abuse prevention
- Detection and deterrence of money laundering, terrorism financing, and other illicit activities
- Behavioral sensors to identify emerging threats and correlate suspicious behaviors
- Fast forensics to integrate text, audio, and visual data sources
- Surveillance tools for early detection and identification of data anomalies, errors, and omissions
- Data quality assurance and compliance with federal and state financial regulatory requirements.

Customers depend on us for effective analytics to ensure early detection of potential price manipulation. Our fraud detection and prevention systems identify data anomalies, errors and omissions, and provide risk profile and impact analysis of financial markets.
Geospatial Intelligence serves customers with current and accurate sensing systems, analytics, and decision support.

**Demand Description**

Civil engineers, city planners, facility managers, and emergency responders require current and accurate geospatial information for their areas of interest. The growing focus on resiliency and protection associated with environment, climate, and weather data drives needs for deploying airborne sensors to collect remote sensing information. The information needs to be georeferenced and interoperable with geographic information systems. Domain expertise is required for acquisition of high caliber data, modeling and analysis, and effective exploitation to derive essential intelligence to inform decisions needed for public safety and security.

**Offering Description**

Northrop Grumman applies our geospatial intelligence domain expertise on customer challenges ranging from aviation safety to water management. We use a suite of remote sensing systems to acquire current and accurate mapping and monitoring data. We manage high volume and velocity solutions for our customers’ geospatial intelligence data. We apply advanced analytics to identify and locate areas where actions need to be taken to ensure public safety and security. We use interoperable standards-based geospatial information architectures to make it easy to integrate with existing customer IT infrastructure.

Northrop Grumman photogrammetric services include airborne imaging, surveying, and mapping. Our airborne acquisition capabilities use advanced sensor systems including high resolution optical cameras, LiDAR, and synthetic aperture radar (SAR). Our solutions enhance applications through superior intelligence gathering. Our mission planning, routing and logistics, and execution monitoring ensure quality data products. We support physical asset tracking, exploration of “what if” scenarios, and data exploitation via advanced analytics and dissemination. We use highly integrated databases and sensor networks and secure systems to ensure the right data gets to the right people at the right time. We provide customers with relevant solutions to ensure full interoperability and control in the world of geospatial intelligence. Our goal is our customer’s mission success.

Northrop Grumman's domain expertise stems from a long history of providing quality aerial imagery, LiDAR, SAR, mapping, imagery analysis, surveying, geographic information systems (GIS), Geospatial Intelligence, and consulting services. Our products and services are used for domestic and international civilian, defense, and intelligence projects. We support public and private sector infrastructure with geospatial intelligence used to better understand the land and its resources.
Decision Support systems enable people to accomplish their missions through effective use of computer-based information coupled with domain expertise.

**Demand Description**
People count on quality information to make timely decisions affecting safety and security. People need computer-based decision support systems when numerous factors must be taken into account and time is limited. Key factors driving critical decision support systems include:

- Accommodation of multiple, large data streams with disparate types of information
- Quick response times requiring fast assimilation and processing of data and information
- Multiple metrics need to be visualized to identify and correlate trends
- Alarms need to go off when data values exceed set thresholds
- Open architectures to accommodate available system components.

**Offering Description**
Northrop Grumman delivers proven decision support systems and tools to reliably assimilate disparate data sources and display key information on dashboards. We have experience in tailoring dashboards to support the people who make informed decisions to serve their mission. We use agile systems engineering and innovative operations centers to develop enterprise solutions for our federal agencies and commercial customers. We employ expert systems with machine-to-machine network technologies and rigorously tested and validated smart logic. We use open source Service Oriented Architectures (SOAs) to enable maximum flexibility to accommodate available components from the global supply chain.

From our Power Grid Dashboard for efficient energy management on Navy facility microgrids to Integrated Health Analytics Platform (iHAP) system for public health officials, Northrop Grumman has designed, integrated, tested, and deployed critical decision support systems for the United States and its allies.

Northrop Grumman decision support solutions serve city, state, national and regional planners, policymakers, and stakeholders. Our tools provide actionable information to optimize safety, security, response, planning, and management of resources. We support customers in addressing regulatory reporting requirements for environmental issues, such as depletion of natural resources. We provide solutions to complex problems involving dynamic interactions between the environment and socioeconomic factors. The Northrop Grumman Decision Support suite blends appropriate modeling & simulation with socioeconomic impacts, regulatory requirements, and direct user feedback.

We support communication-driven, data-driven, document-driven, knowledge-driven, and model-driven decision support systems. We tailor decision support to meet the needs of each customer and their mission.
Healthcare Fraud Prevention

Analytic approaches to identify and help prevent improper payments, fraud and abuse.

Fraud prevention is critical for limiting waste, abuse, and the improper allocation of limited healthcare resources.

Demand Description
Fraud, waste and abuse drive up costs for everyone in the healthcare system, in addition to hurting the long-term solvency of the Federal health care programs upon which millions of Americans depend. When families are working to make every dollar count, eliminating waste, fraud and abuse must be a top priority. Northrop Grumman supports Healthcare Fraud Prevention for the Centers for Medicare & Medicaid Services (CMS) to ensure correct payments are made to legitimate providers for covered, appropriate, and reasonable health care services.

Offering Description
Northrop Grumman supports the Centers for Medicare & Medicaid Services’ (CMS) National Fraud Prevention Program in their mission to prevent and detect fraud, waste, abuse, and other improper payments under the Medicare program, and CMS’ vision to implement proven predictive modeling tools into the claims processing system to stop payment on high risk claims.

Northrop Grumman designed, developed, and implemented the system using analytic approaches to generate alerts and evaluate results to identify and help prevent improper payments, fraud and abuse.

Our domain expertise helps decrease healthcare costs, preventing the misuse of taxpayer dollars that can result from waste, fraud, and abuse of the Medicare program. Our uniquely qualified team utilizes proven solutions and industry best practices to help prevent fraudulent transactions before they occur, rather than identify fraudulent activity after the fact.

Our support for the fraud detection program includes:
- Real-time analysis of healthcare markets for fraud indicators, risk profile and potential impact
- Proactive data mining, fusion and predictive analytics for fraud, waste, and abuse prevention
- Behavioral sensors to identify emerging threats and correlate suspicious behaviors
- Surveillance tools for early detection and identification of data anomalies, errors and omissions
- Data quality assurance and compliance with federal and state financial regulatory requirements.
For land, sea, air and space, Northrop Grumman is a recognized leader in unmanned systems. The depth and breadth of our platforms and technologies portfolio provide customers with a wide range of capabilities to serve their missions.

**Demand Description**

Unmanned systems are needed to operate in high threat areas, to conduct extended missions, and to reduce risks to human lives and national security. There are increasing needs for airborne, spaceborne, land-based, and underwater unmanned systems with a wide range of capabilities.

**Offering Description**

Northrop Grumman offers a family of unmanned systems to meet a wide range of mission requirements.

**Global Hawk**

Global Hawks provide intelligence, surveillance, and reconnaissance collection to support security forces worldwide. The systems support civil and commercial customers in conducting border patrol, port surveillance, hurricane monitoring, disaster relief support, and high-altitude scientific research. The systems complement manned and space reconnaissance systems by providing near-real-time coverage using radar, imagery intelligence (IMINT) sensors, signals intelligence (SIGINT), and communications relay.

**Bat**

Bat is an affordable, medium altitude, multi-mission platform. Bats are configured with different-sized fuel tanks and sensor payloads to meet a range of tactical missions, including intelligence, surveillance, reconnaissance, target acquisition, and communications relay. Bat has a blended body design, enabling a much larger payload volume of 3.2 cubic feet to carry more payload than other unmanned vehicles of its size.

**Firebird**

Firebird is an open architecture payload in an optionally-piloted aircraft. The easily configured platform accommodates multiple intelligence, surveillance, reconnaissance (ISR) and communications sensor payloads to provide real-time data collection. The Firebird platform information management tools enable users to easily exploit data to make decisions.

**Fire Scout**

Fire Scout vertical takeoff and landing (VTOL) provides unprecedented situational awareness and precision targeting support for U.S. Armed Forces. Fire Scout is based on a commercial airframe with over 20 million flight hours and incorporates proven, reliable turbine power with 160 million flight hours.
The capability to integrate a set of products and capabilities from multiple companies into a single system has never been more important to mission success than it is today.

**Demand Description**

Enterprise-wide systems need effective integration. Users depend on complex, integrated systems to affordably, reliably and securely serve their missions. Key drivers for high-caliber systems integration include:

- Need for affordable life cycle costs drive expectations for low operation and maintenance costs
- All functions and subsystems need to meet operational requirements, all the time
- Systems need to be reliable under a wide range of operating conditions
- Open architectures need to accommodate plug & play components
- Agile systems development for sustained operations and incremental capability to serve missions.

**Offering Description**

Northrop Grumman delivers proven systems integration processes tools to intelligently integrate subsystems into reliable and secure operational assets. We have experience in bringing together commercial products with tailored technologies to meet the rigorous demands of our customers. We use agile systems engineering and large-scale network management and operations centers to serve commercial enterprises and federal agencies. We employ dynamic, extensible enterprise systems tailored and scaled for each application. We use open architectures to enable maximum flexibility and optimize a high quality global supply chain.

From UAVs for the Air Force and Navy, to Command, Control, Computing, Communications, Intelligence, Surveillance, Reconnaissance (C4ISR) solutions to the Cyber Security Operations Centers (CSOCS) and Integrated Health Analytics Platform (iHAP) system, Northrop Grumman has designed, integrated, field tested, and deployed critical infrastructure for the United States and its allies.

Northrop Grumman has more than 40 top-level ratings for benchmarking commercial and defense industry best practices for management and engineering, validating the company’s number-one ranking as a federal systems integrator. The Software Engineering Institute developed the Capability Maturity Model Integration (CMMI) rating system to objectively assess the full range of an organization’s software and systems engineering, program management, and organizational management capabilities. Northrop Grumman has achieved the highest level CMMI rating of “5.” The CMMI 5 rating signifies lower risks to successful program execution.
Complex, technical missions need trained personnel to effectively and safely conduct operations. Northrop Grumman has domain expertise to train and equip technical teams to serve the security of their enterprise.

Demand Description
Efficient and effective operations drive demand for tailored technical training and interactive data support integrated through a common, reliable, and trusted source to provide on-demand, 24/7 availability.

Offering Description
Northrop Grumman offers domain expertise integrated into technical training through the Training and Technical Resources Integrated Performance Support System (TRIPSS). TRIPSS is a standards-based, database-driven system with options to be networked or used as a stand-alone system. People can use TRIPSS on desktops, laptops, and tablets running on Windows (XP, Vista, and Win7), Android (2.2+), MAC OS, and iOS.

TRIPSS’ high-end graphical interface allows users to access a suite of tailored training tools including:
- 3D Modeling of Systems, Subsystems, and Components through a graphical, interactive method describing component location and functionality
- Computer-Based Training (CBT) with integrated training simulations and assessments
- Interactive Job Aids combine step-by-step procedures with 3D animations created from official computer-aided design (CAD) drawings
- xSync Video Training provides anytime access to instructor-led training
- Course Tracking System (CTS) tracks and reports training status
- Interactive Electronic Technical Manual (IETM) for Technical Documentation/Technical Orders
- Document and Media Archive for any media format
- Quick Reference Guides

TRIPSS – Key Benefits
- Lowers recurring training cost
- Provides students with a “go at your own pace” interactive training
- Includes options for standalone training, in-class training tool, and an on-the-job refresher/reference tool
- Increases student comprehension and knowledge retention for complex concepts and tasks
- Provides managers with a Course Tracking tool for assigning courses and for assessing and reporting student progress
- Allows operators anytime-access to role and task-based training, interactive system breakdowns, procedural steps and interactive 3D system components, engineering drawings, and program/product documents
- Provides a one-source, on-demand, searchable library of all training and technical support data for system operations and maintenance
- Complies with DoD standards and requirements
Northrop Grumman Global Security

PRODUCTS

Products and Services to meet Physical Security needs

- SecureSite
- SecureC4
- SecureCyber
- SecureEnergy
- SecureEnvironment
- SecureHealth
- SecureData
SecureSite Product Overviews

- **Tailorable Integrated Security Solutions - TISS™**
  - Critical Infrastructure Perimeter Security System

- **Integrated Base Defense Security System - IBDSS™**
  - Security System for Defending an Enterprise Base

- **Expeditionary Tactical Automated Security System - ExTASS™**
  - Deployable Security System

- **Harbor & Coastal Security - HCS**
  - Harbor and Coastal Security System
Tailorable Integrated Security Solutions (TISS\textsuperscript{TM})

Critical Infrastructure Perimeter Security System

TISS\textsuperscript{TM} extends detection and assessment capabilities far beyond the site perimeter via a modular, expandable, and seamless physical security monitoring system.

**Demand Description**

Many organizations rely on multiple, stand-alone security systems to control access and to protect their facilities. These systems do not share information and cannot provide a complete picture of a site’s security posture. Today’s threats demand integrated security solutions to deliver complete situational awareness.

**Offering Description**

Northrop Grumman’s integrated, state-of-the-art security solution is TISS\textsuperscript{TM}. TISS\textsuperscript{TM} extends detection and assessment capabilities far beyond the site perimeter. Earlier detection enables earlier assessments, which in turn maximizes response timelines for security personnel.

**Tailoring Solutions for Critical Infrastructure**

Powerful TISS\textsuperscript{TM} tools enable operators to simultaneously manage and oversee multiple sites with critical infrastructure assets, such as airports, seaports, chemical plants, pipelines, railways, refineries, power plants, dams, and waterways. Operators can assign supervisory responsibilities for any site, from any site. Camera controls can be easily granted to any operator on the network. TISS\textsuperscript{TM} is modular, expandable, and integrates legacy security systems with state-of-the-art detection and assessment security technologies into one seamless system.

**TISS\textsuperscript{TM} Benefits**

TISS enterprise-wide solutions are based on an open architecture to be flexible and scalable. Each site installation is unique, based on perimeter size, topography, sensor suite, and other local factors. TISS\textsuperscript{TM} brings security benefits to each site:

- **Simplicity for Reduced Training Costs** - Operators interface with one system
- **Improved Situational Awareness** - Correlates input from multiple sensors before displaying “actionable” data.
- **Improved Operational Effectiveness** - Supports a layered defense capability, raising the probability of accurate detection, while reducing false and nuisance alarm rates.
- **Reduced Manpower Requirements** - Synergizes electronic “eyes” from various detection and assessment devices into a comprehensive picture.
- **Reduced Life-Cycle Costs** - Integrates in-place security systems, leveraging investments, and allows new devices to be added easily.

**Northrop Grumman – A Proven Leader in Site Security**

TISS\textsuperscript{TM} is tested, fielded and operational, providing a simple and scalable solution to growing with the customer’s needs over time. The ability to tailor the security solution based on changing security priorities increases the availability of security options.
Integrated Base Defense Security System (IBDSS™)

Base Security System

Integrated Base Defense Security System (IBDSS™) automates detection, assessment, response and delay or denial of physical breaches.

Demand Description

Government and military organizations have relied on stove-pipe security systems to protect facilities and restrict unauthorized access. Today’s threats demand integrated solutions to make comprehensive assessments and direct rapid responses.

Offering Description

Northrop Grumman assists defense and civilian agencies in designing, implementing, supporting, and enhancing physical security solutions around the globe.

Using a network-centric architecture, IBDSS™ offers flexible, scalable, enterprise wide security, with the needed level of integration to meet operational requirements.

Command and Control (C2)

The core of the IBDSS™ is command and control. Our C2 solution provides an integrated operational picture of the monitored area and synchronizes data dissemination across a wide variety of clients, enabling peer-to-peer communications.

IBDSS™ automates detection, assessment, response and delay or denial of physical breaches by integrating:

• Wide Area & Perimeter Detection sensors
• Integrated Long- and Short-range Assessment cameras
• Access Control devices, and
• Entry Delay/Denial systems

IBDSS™ enables more rapid human assessment and response times using machine-to-machine integrated detection and assessment. The result is more effective use of security forces, maximizing detection accuracy and minimizing false alarms.

IBDSS™ correlates multiple sensor inputs before displaying “actionable” data – a truly “smart” capability. IBDSS™ provides a common operational picture and real-time data and information sharing.

Northrop Grumman – Trusted Partner for Integrated Site Protection

Northrop Grumman uses domain expertise to provide best-in-class solutions, coupled with cutting-edge security technologies, integrated with legacy components. We work with leading vendors in the physical security industry to meet evolving requirements and develop interface specifications.

Our technology expertise includes:

• Smart Sensors, Data Fusion, C2 Integration
• CCTV and Enhanced Video Detection
• Ground Based Radar
• Unattended Air and Ground Vehicles
• Remotely Operated Weapons
• Chemical and Biological Sensors
• Biometric Readers and Trackers
• Satellite Tracking and Communication Systems
Expeditionary Tactical Automated Security System (ExTASS™)

**Deployable Security System**

**ExTASS™** is a tactical, light-weight, rapidly deployable, all-weather force protection asset designed to provide perimeter security in both expeditionary and fixed-site scenarios.

**Demand Description**
Mobile sites need portable solutions for border and perimeter security able to be easily deployed on rugged, light-weight, and consolidated platforms for storing and deploying sensor suites.

**Offering Description**
A fully outfitted ExTASS™ trailer can be deployed in under 30 minutes, allowing mobile forces to quickly secure a perimeter. The trailer can be configured with an installation specific selection of equipment from over 150 commercial and military electro-optical/infrared cameras, ground-based radars and sensors. Situational awareness is provided by state-of-the-art software. The on-board server and wireless communication link allow ExTASS™ to operate as a stand-alone system or as a larger security network capable of simultaneously transmitting video, targets, radar detections and assessment information back to a centralized operations center.

**Features**
- Short, Medium, Long, and Ultra-Long Range Camera Capabilities
- Multi-Range Ground Surveillance Radars
- Seismic, Beam-Break, Fence-Shake, and Acoustic Sensors
- Light-Weight, Rugged Trailer
- Auto-Leveling 30’ Mast
- 3kW Diesel Generator with Battery Bank
- Local Wi-Fi Network Radio and High Bandwidth Point-to-Point Radio
- Map Client and Digital Video Panel for Situational Awareness and Camera Viewing/Control
- All-Weather Enclosure
- Storage for Sensors, Cameras, Tools

**Benefits**
- Networked Situational Awareness with Alarm Management
- Standalone or Multi-Trailer, Networked Operation
- Flexible System Architecture: Easily Integrate Additional Cameras and Sensors
- Environmentally Hardened
- Low Maintenance & Easy to Use
- Integrated with Higher Echelon Systems
- Remote User Interfaces
- Flexible Power Solution

**Command & Control Features**
- Camera and sensor control from local tower, any networked tower, or a remote operation center
- Slew-to-cue camera control for immediate target assessment
- Simultaneous target updates on all networked clients
- Assess targets and update locations in real time with cameras equipped with laser range finders
- Video forensics tools to search and export all video based on time and geographical area
- Highly optimized user interface allows operator to assess video and targets from multiple towers
Harbor and Coastal Surveillance (HCS)

Harbor and Coastal Security System

H
arbor and Coastal Surveillance System supports operations for layered, multi-agency maritime security, safety, and environmental protection.

Demand Description

Ports and harbors dealing with multiple threat vectors need integrated solutions with automated collection, analysis and dissemination of information essential to maritime operations for:

• Coastal Surveillance and Security
• Port and Harbor Security
• Vessel Traffic Management
• Anti-Terrorist Force Protection
• Interdiction and Response

Offering Description

Northrop Grumman’s HCS system integrates off-the-shelf computers, communications, and sensors with sensor processing and databases to form a flexible, standards-based, service oriented architecture to provide:

• Integrated video, radar, and Automatic Identification System (AIS) surveillance
• Multi-source, multi-sensor correlation
• Vessel, aircraft, people
• Transit and route management
• Zone management
• Alarms and alerts
• Rule-based anomaly detection
• Secure and unsecure AIS data

The foundation for HCS is the Northrop Grumman Interoperable C4I Services (ICS) software product, a commercial variant of software for a DoD family of systems. The ICS architecture provides core services including track management, data communications, situation display, and decision aids.

Sensor and Data Integrations

For continuous surveillance, HCS utilizes a network of interlinked sensors including AIS, medium and long-range optical and infrared cameras, medium range harbor and approach radars, and long-range high performance coastal radars. HCS can receive external sensor data via web services and standardized interfaces to commercial and military radars, Long Range Identification and Tracking (LRIT), satellite and terrestrial based AIS, and tactical data links.

HCS databases contain extensive information about vessels, aircraft, movements, standard routes, cargo, crew and passengers. The databases can be populated and updated from commercial sources such as Lloyds or government agencies such as the Coast Guard, Navy, and Customs.

Benefits

HCS performs automatic correlation and association of tracks with database information, resulting in a common operational picture (COP).

HCS is easily adapted and scaled for shore-based, offshore or shipboard use, and can serve as a standalone system or be utilized in a systems-of-systems architecture, providing layered support across multiple missions and agencies.
SecureC4 Product Overviews

- **Integrated - Joint Operational Command and Control Services (I-JOCCSTM)**
  - Monitoring and Operations for Security & Safety

- **Law Enforcement Information Exchange (LInX)**
  - Law Enforcement Information Exchange

- **CommandPoint™**
  - Public Safety Information Suite

- **Public Safety Broadband Wireless**
  - Ensured Communication for Critical services

- **Airport Real-time Collaboration™ (ARC)**
  - Effectively Managing the Flow of People Through Airports
Integrated - Joint Operational Command and Control Services (I-JOCCSTM) provides facility managers with integrated information system solutions for monitoring and operations to maximize security and safety.

Demand Description
Facility managers need effective monitoring and management tools to maintain situational awareness over all dimensions of site operations. All of the critical input associated with safety and security need to be tied into a single Command and Control (C2) center. C2 is essential to enable all layers of the operations to communicate and collaborate, especially associated with threat avoidance and response.

Offering Description
I-JOCCSTM is a high caliber, secure and user friendly solution. Solutions can be deployed for fixed site installations and remote operators. Cross-domain security enables integration of all security, safety and mission assurance systems.

The flexibility of the I-JOCCSTM architecture serves specific customer needs. Our solutions use commercial off-the-shelf (COTS) products combined with ‘in-house’ engineering expertise integrated with existing facility processes and systems. Our extensible architecture allows third-party applications to be incorporated to deliver mission-specific services.

I-JOCCSTM is scalable to meet the full range of deployment options from small to large facilities. The capability offers Facility Operations, Track Management, Communications, Data Correlation, Intelligence Collation, Geographic Displays, Visualization, Decision Aids and Planning Tools.

I-JOCCSTM incorporates a number of technologies within a Service Oriented Architecture (SOA), including:
- Open Geospatial Consortium (OGC) Compliant Web Mapping Services
- Web Portal
- Messaging infrastructure
- Federated identity management and security

Features
- Cost-effective solution for integrated situational awareness and C2
- Core systems in service with 40 nations including United Kingdom and United States
- Low cost life cycle sustainment using proven standards
- Extensible and evolvable architecture

Benefits
- Robust, military-proven capability supporting US Joint Forces
- Common Operating Picture (COP) derived from multiple, distributed sources
- Information intelligence and planning throughout the facility or enterprise
- Intuitive Human Machine Interface (HMI)
- Interoperable with principal facility systems
The Law Enforcement Information Exchange, or LInX, is a regional information sharing system created, coordinated, and primarily funded by the U.S. Naval Criminal Investigative Service (NCIS). It has begun to revolutionize law enforcement in the 21st century.

Demand Description

In today’s digital environment, information is more important than ever for the patrol officers, investigators, and crime analysts supporting our communities. The days of “information is power” or “my information, my case” are behind us as a law enforcement community. The tragic events of 9/11 and subsequent violent assaults in our high schools and universities across the nation prove more than ever that we, as a law enforcement community, are inter-dependent. We must move to a new paradigm, one characterized by willingly and necessarily sharing information, cases and records. The criminals and terrorists who attack the citizens who we are sworn to protect, exploit our jurisdictions and borders to their advantage. It is time we take any advantage away from them through prudent, secure and responsible sharing of law enforcement information.

Offering Description

LInX breaks down artificial jurisdictional and technical barriers between municipal, county, state, and federal law enforcement agencies. This state-of-the-art collaborative information sharing program is currently operating in ten regional locations around the U.S. along with the Department of Defense Information Exchange which provides LInX services for the DoD law enforcement agencies. According to NCIS statistics, over 1300 law enforcement agencies are using LInX in their daily routines, and more than 38,000 law enforcement professionals have been trained in and are employing LInX to achieve investigative and operational successes. Virginia law enforcement agencies alone query LInX more than 120,000 times each month.

Having current information available at the street level has enhanced officer safety and the ability to solve crimes, fight terrorism and protect strategic assets. The ability to instantly retrieve relevant data on people with whom the officer is in contact, or is about to contact—data contributed by other law enforcement professionals who have histories with the subject—is making our law enforcement environment safer each day. Tactics and strategies can be developed and approached from a position of greatly improved knowledge of the subjects, their potential locations, associates, vehicles and past habits.

LInX is a proven operational capability in those regions where it has been deployed. LInX and similar information-sharing initiatives must be encouraged by executive law enforcement leadership, and institutionalized in the same way we have become dependent upon fingerprinting and DNA analysis.
CommandPoint™ is the latest evolution in public safety systems application suites from Northrop Grumman. The CommandPoint™ application suite combines the best technological standards with five decades of Northrop Grumman experience.

Demand Description
Emergency responders need the timeliness of computer-aided dispatch, the efficiency of automated field reports, on-line access to all public safety records management, all coupled with the ability to map real-time command and control.

Offering Description
CommandPoint™ uses a true Windows interface, making it among the most streamlined products in the public safety market. The CommandPoint™ suite of products is user-configurable and easy for both the casual or experienced user. In the computer-aided dispatch (CAD) application, status monitors are completely configurable by the user, and allow features such as sorting of information, defining user specific monitors, and monitor placement, all designed for more effective use of unit and activity data.

CommandPoint™ is much more than an integrated first responder application suite. CommandPoint™ is a full-spectrum approach using the latest technology in a robust, cost-effective, and maintainable solution.

CommandPoint™ Suite Includes the following applications:

- **CommandPoint CAD (Computer Aided Dispatch):** The command and control system for public safety, computer-aided dispatching and resource management with multi-agency scalability, configurable user preferences, increased speed in execution of commands, and collapsible windows.

- **CommandPoint Mobile:** The application interface between the CAD system and the field units provides efficient dispatching and status of field units and ease of use in accessing data with a flexible easy-to-use display, simple & user-friendly terminal-to-terminal messaging, as well as precise and convenient dispatch notification.

- **AFR:** An automated field reporting package that enables law enforcement units to complete reports quickly and accurately, thus increasing their time in the field.

- **MAP:** The mapping application designed for real-time command and control situations supporting Automatic Vehicle Routing and Recommendation (AVRR)/Automatic Vehicle Location (AVL).

- **Law Enforcement RMS:** A law enforcement records management system utilizing the latest in technology to get information into and out of the system to assist in better decision making.

- **Fire RMS:** A fire records management system that provides ease of use in collecting, sorting, and managing data for fire reports, inspections, and National File Incident Reporting System (NFIRS) reporting.
Public Safety Broadband Wireless provides emergency managers with the ability to communicate critical information to first responders, in real-time, and across jurisdictional boundaries.

**Demand Description**
Advances in wireless technologies have the potential to transform public safety and operational execution. Third generation (3G) and fourth generation (4G) mobile broadband wireless technologies can significantly advance the operational capabilities of public safety by enabling a variety of mission-enhancing applications including video streaming and surveillance, location based services, and license plate readers.

**Offering Description**
Northrop Grumman engineered, designed and deployed a highly reliable and secure 3G broadband wireless network for the city of New York, called NYCWiN. NYCWiN expanded the City’s existing infrastructure to provide a multiagency broadband communications capability for the city to mobilize its workforce, deliver real-time information to first responders, and enhance situational awareness with real-time monitoring and management capability.

NYCWiN continues to demonstrate its value to the city’s public safety operations by integrating customized mission applications at more than 40 city agencies serving secondary responders, with more agencies added every day. Some of these applications include: remote traffic control, mobile inspections, sensor management, wireless video, license plate recognition, wireless meter reading, emergency call boxes, and automatic vehicle location (AVL).

**FirstNet**
Northrop Grumman Public Safety Broadband Wireless can serve FirstNet Nationwide Network (FNN) as critical infrastructure to provide first responders unprecedented connectivity with critical tools, including data and information, videos, maps, schematics and real-time status updates, while preserving security and reliability.

The network allows public safety individuals to respond to rescue operations, emergencies, and every day public protection missions quickly, and all access to secure system information immediately at the municipal, state or federal level. The network characteristics include:

- Transformational communications for first responders
- High reliability during the most extreme circumstances
- 4G LTE technology implemented with public safety specific requirements
- Improved/enhanced operational efficiencies with new apps
- Protected as a National Critical Infrastructure (NCI) component
- Cybersecurity protection subsequent with the requirements of law enforcement, health, and civil agencies
Airport Realtime Collaboration (ARC)

Collaborating to Create a Great Passenger Experience

**Demand Description**

Airports require a comprehensive portfolio of software products and services to support realtime collaboration. Improved efficiencies to airside and terminal operations, improved planning and flow-through security, and support for retail operations through provision of accurate forecasts and live passenger movement data can drastically increase the operating efficiency of an airport.

**Offering Description**

The ARC portfolio is made up of:

- ARC Airport Collaborative Decision Making (A-CDM)
- ARC Passenger Flow
- ARC Analytics
- ARC Professional Services

ARC’s passenger flow module is unlike the people-tracking systems currently deployed in some airports. Based on a sophisticated artificial intelligence capability which simple counting and tracking systems lack, ARC can genuinely improve forecasting capability and provide timely live updates allowing proactive, even pre-emptive, management of passenger movements. This can benefit the airport in several areas:

- More accurate and detailed seasonal forecasting for planning and rostering
- Forecasting of numbers and dwell times in departures for retail planning
- Optimum resource planning to minimize queues while retaining cost control
- Live updates to forecasts and alerts if actual numbers deviate from the forecast – for example giving a 45-60 minute warning ahead of any surge in passengers at security
- All types of people-counting systems can usefully feed into ARC Passenger Flow to validate the forecast the system produces.

Airport Collaborative Decision Making (A-CDM) can revolutionize the airport’s operation, bringing shorter taxi times, fewer and shorter delays, reduced fuel burn and CO2 emissions providing an altogether more efficient way of working.

ARC A-CDM modules include:

- **Groundview** – ground radar display available to all A-CDM partners (air traffic controllers, airport operations, airlines) for shared situational awareness
- **Flightview** – flight information, turnaround data and A-CDM milestones in a shared view
- **Predeparture sequencing** – Target Start-up Approval Time (TSAT) calculation and optimum sequencing based on accurate input of Target Off-Block Time (TOBT) and Variable
SecureCyber Product Overviews

- **Advanced Malware Platform (AMP) - Dynamic Email Protection**
  - Protection and Prevention

- **CSOC - Cybersecurity Operations Center**
  - Persistent Network Monitoring

- **CyberSpace Solutions Center**
  - Full Spectrum of Cyber Operations - For Times of Peace or Conflict

- **SPIDA™**
  - Network Security to SCADA Environments
Advanced Malware Platform (AMP) - Dynamic Email Protection

Protection and Prevention

Advanced Malware Platform (AMP) reduces risk on the enterprise network by dynamic detection of advanced persistent threats (APTs) and zero-days.

Demand Description

APT and zero-day malware attacks cause significant damage before they are detected and countermeasures established. Most commercially available intrusion detection systems use signatures which are not effective in detecting APT and zero-day attacks. Currently, network defenders characterize network intrusion as the “80/20” rule: 80% of intrusions are traditional malware-based; 20% are APT, where traditional security defenses and incident response are largely ineffective. As a result, targeted spear-phishing email employing zero-day exploits render signature-based network defense efforts largely ineffective.

Offering Description

Northrop Grumman offers an advanced malware detection platform based on an innovative multi-injection sandbox and malware risk-scoring engine using both custom and COTS-based malware detection and analysis technologies.

AMP is a proactive approach to directly address APT email-based intrusions. It is a continuous malware processing architecture that actively detects and blocks spear-phishing attacks in real-time, while performing risk based scoring and actionable reporting within an integrated knowledgebase. AMP is a truly unique “outside the box approach” to APT malware detection based on five key innovations:

- **Full Automation** – No “operator in the loop” workflow processing hundreds of email attachments and web-links per hour
- **Multiple Injection Sandboxes** – Run multiple instances of malware analysis tools in a fully integrated secure virtual environment
- **Adaptive Behavior-Based Detection** – Automatically detects, learns, and adapts to suspicious and unauthorized activity using machine learning classifiers in a trusted environment
- **Risk-Scoring Engine** – Robust logic and risk scoring engines quantify anomalous file activity in real-time
- **Malware Data Warehouse** – A data warehouse that contains a knowledge base to support decision-making for actionable cyber threat intelligence

Advanced Malware Platform – Reduces Risk

AMP reduces risk on the enterprise network by dynamic detection of APTs and zero-days. AMP contributes to situational understanding and the over-all threat “heat-map” of the network. It dynamically protects network endpoints via the multiple injection sandbox technology using integrated malware analysis tool processing. AMP should be in the tool arsenal for all Security Operation Centers, Critical Incident Response Teams and Focused Operations teams.
Cyber Security Operations Center is dedicated to protecting Northrop Grumman’s Global Network and its customers’ networks and intellectual property through intelligence collection and fusion, threat detection, incident response, digital forensics, and 24/7/365 security monitoring.

**Demand Description**

Cyber attacks by nation-state threat actors, hostile adversary organizations, and organized crime are on the rise, threatening governments, corporations, and individuals by attempting to extract technical, financial, strategic, and national security information. Increasingly sophisticated and aggressive methods used in these attacks require that equally dedicated measures be taken to detect, respond, and adapt quickly to new cyber threats in order to protect critical information assets.

**Offering Description**

By combining the latest cybersecurity technologies with domain expertise in information security and intelligence operations, Northrop Grumman’s Information Security organization has created a state of the art Cyber Security Operations Center (CSOC) dedicated to protecting Northrop Grumman’s critical network infrastructure, its customers’ networks and proprietary data through advanced intelligence collection operations, liaison with Defense Industrial Base partners, LE/CI engagements, digital forensics, and security monitoring.

**Identifying and Mitigating Advanced Cyber Threats**

The CSOC blends traditional operational functions (such as security monitoring) with competitive intelligence collection and analysis in a collaborative environment. Additionally, a team of individuals are focused on threat detection through reverse engineering and network forensics. This allows the team to more effectively identify and mitigate advanced cyber threats.

- **Security monitoring**: The CSOC is staffed 24 hours-a-day, seven days a week, providing security monitoring for over 75,000 hosts and 10,000 servers located in the US and Internationally.

- **Incident response**: Handlers respond to suspected security incidents, providing containment of incidents, detailed root-cause analysis and restoration of services.

- **Digital forensics**: Computer forensic examiners collect and analyze evidence from digital media and present their findings in reports that are admissible in court.

- **Advanced Technical Solutions Team**: A highly technical team of operators develop and deploy solutions.

- **Advanced Threat Analysis Center**: Network forensic/intelligence operators analyze terabytes of data daily to identify and mitigate internal and external threats.

- **Strategic CounterIntelligence Team**: A team of individuals dedicated to analyzing the long range cyber threat to NG and its partners.

**Broad Range of Security Solutions**

Through the effective and unique use of COTS and proprietary solutions NG has the ability to fit your cybersecurity needs from 24/7/365 monitoring to advanced data analytics and network forensics.
CyberSpace Solutions Center (CSSC) enables the full spectrum of operations for times of peace or conflict.

**Demand Description**

Hostile attempts to penetrate networks are a fact-of-life across government and commercial enterprises. Threats span nuisance attacks to denial of service, disruption, theft, fraud, and cyber-enabled infrastructure destruction. The impact of data loss and its associated monetary loss increases daily. Today’s government and commercial enterprises cannot function without effective cybersecurity solutions.

Developing defensive and full spectrum cyber solutions requires people, processes, and technology to deliver capability from concept to deployment. Minimum lifecycle cyber-solution support needs include:

- Concept development
- Range instrumentation
- Modeling and simulation
- Experimentation
- System integration
- Planning
- Exercising
- Mission execution

**Offering Description**

The Northrop Grumman CSSC is an adaptable and scalable resource that can host teams of network defenders and full spectrum operators to rapidly develop, integrate, test, and deploy experimental, exercise, or mission capability. The CSSC provides cyber developers and operators the ability to develop, exercise and perfect tactics, techniques and procedures in a faithfully replicated network enterprise. Accurate emulation allows realistic, “live-fire” penetration and preventive operations to be conducted safely and legally; segregated from actual operational networks.

These capabilities range from simple network operations, such as logging anomalies, correlating attack information and reacting to adversary actions, to a more proactive stance that assures organizations withstand attack and continue their missions and services.

**CSSC – Adding Value to Cyber Operations with Effectiveness Across the Entire Spectrum of Conflict**

- Peacetime preparation helps deter hostilities and ensures readiness
- Training and exercising in a safe, realistic environment
- Applicable to network defense, exploitation and attack
- Relevant for civil, federal, defense and commercial purposes

For over a decade, Northrop Grumman has been actively involved in creating capabilities and supporting cybersecurity professionals - efforts began with small, separate, distributed capabilities and have evolved into an extensive, distributed, net-centric cyber environment.
SPIDA™ is high-grade network security for Supervisory Control and Data Acquisition (SCADA) environments for industries including mining, oil and gas, water, food production, energy, and manufacturing.

**Offering Description**

The M5-SPIDA™ solution encompasses both central and distributed elements of the SCADA network, including interfaces to enterprise networks. Compact and rugged, the M5-SPIDA™ has been designed for use in harsh industrial environments. Direct simultaneous connections to public and private IP carriers are supported, along with comprehensive routing functionality. This removes the need for additional external network components. Configuration and centralized management of the M5-SPIDA™ is provided via an easy-to-use touch screen interface utilizing icon driven menus, rather than an unfriendly command line interface.

This substantially reduces the training required to understand, deploy and operate the solution. Importantly, the M5-SPIDA™ further strengthens an array of built-in security features by integrating Snort™, the market leading advanced intrusion detection system by Sourcefire™.

**Features Description**

- Secures SCADA networks from cyber attacks and subversion attempts
- Enhanced by the Snort™ intrusion detection system (IDS) engine, open rule language with third-party signature support
- Integrated support for public/private IP networks such as SPIDA™
- Secure remote connection to local scada network satellite, 3G and 4G, wireless and ethernet
- Comprehensive remote administration and monitoring capability
- Lightweight and rugged
- Integrated support for common SCADA protocols like Modbus (TCP) and OPC
- Provides secure encrypted VPN connectivity to SCADA network
- Easily customizable connectivity options to suit available services at remote locations
- Integrates with the Sourcefire™ family of products and features (RNA, PAT, RUA, DC)
- Provides secure remote access for field engineers, vendor support contractors, and support staff
- Suitable for use in industries including energy sector, ports and harbor security, cities and states, international critical infrastructure security, and manufacturing industries
SecureEnergy Product Overviews

- **Power Grid Dashboard™**
  - Secure & Sure Power Grid Monitoring

- **PowerGrid**
  - Highly Versatile, Feature Rich, Tough, and Small

- **SCADA Protocol Unique Digital Signature (SPUDS™)**
  - SCADA Protocol Unique Digital Signature (SPUDS) Tool
Power Grid Dashboard™ provides energy managers with an effective web-based monitoring system to help energy managers make informed and timely decisions based on empirical data.

Demand Description
Energy managers demand an effective monitoring system to make informed power-routing decisions based on trusted, real-time data pulled from disparate sources. They need energy generation and consumption data in an actionable format to allow them to make time-critical decisions more quickly and with greater confidence, avoiding potential errors and increasing energy efficiency.

Offering Description
Northrop Grumman’s Power Grid Dashboard™ provides an effective web-based monitoring system to help energy managers make informed and timely decisions based on empirical data from a variety of disparate data sources including renewable energy sources, operational load data from building management systems, utility grid power, diesel generators, and electric vehicle charging systems. By tracking generation and consumption sources, the Power Grid Dashboard™ allows energy managers to optimize power usage and reduce overall energy costs.

The Power Grid Dashboard™ is based on a flexible and scalable framework mapping disparate data streams to a common data format. Brokering of information based on a “plug-in” architecture allows an extensible and uniform approach to handling data and services. Designed with an open API (allowing developers to build and dynamically upload plug-in components) the framework’s data integration functionality, flexibility, and scalability are extensible. The information broking and data correlation layer aggregates and exposes web service interfaces for importing, exporting, processing, and rendering information. The Power Grid Dashboard™ supports seamless interfaces between client applications and data/service providers to ensure isolation from changes that occur over time. Additional interfaces can be readily incorporated into the Dashboard to allow energy managers to monitor and manage other areas in their network or sphere of regard.

An operational implementation of this energy monitoring system is Northrop Grumman’s Dashboard product for newly constructed barracks on US Marine Base, Camp Pendleton, California. This energy monitoring and management system interfaces with concentrated photovoltaic (CPV) solar arrays, traditional (flat) photovoltaic solar arrays, building HVAC systems, water and natural gas meters, backup diesel generator sets, operational load controllers, and electric vehicle charging stations.
PowerGrid product line represents a modular set of common Uninterrupted Power Supply (UPS) power components that can be configured in a variety of ways to meet nearly any mobile, tactical, or harsh environment application.

**Demand Description**
A range of applications demand lightweight, versatile, reliable, and rugged UPS.

**Offering Description**
Northrop Grumman’s PowerGrid UPS combines the latest advancements in UPS power and battery technology.

**Over-Voltage Design:** Each of the 400 watt inverters in the PowerGrid system is designed to handle 2X over-rating surge or in-rush currents. An 800 watt system will provide up to 1600 watts of over-rating power for short periods of time. The inverters are protected by a set of over-temperature and over-voltage protection circuits that are interlocked so that when the over-temperature circuits sense a breach of the maximum allowable temperature, it enables the over-voltage protection circuit to limit or throttle the maximum allowable power output down to a maximum of 1100 watts. The over-specification of UPS power system is no longer necessary, providing the ability to reduce initial costs, size, and weight of the power support design.

**Primary Power Options – Volts Alternating Current (VAC)/Volts Direct Current (VDC):** PowerGrid has been designed as an “all purpose” ruggedized UPS capable of operating in any environment anywhere in the world. It can be connected and powered by both AC and DC sources and is designed with a unique automatic sensing and power switching capability rarely found in other UPS architectures. PowerGrid is full MIL-1275 compliant for VDC operations including the charging of the battery components.

**Battery Technology – Lithium Polymer Cold Pak:** One of PowerGrid’s most significant design features is its advanced technology battery backup capability. This design provides significantly more energy storage capacity of a normal 23lbs lead acid battery in a small 3lbs battery pack. The dual “Hot Swap” battery packs within each PowerGrid 800 UPS will provide between 6 and 9 minutes of hold time for the attached equipment and, with an attached battery expansion module, will provide over 30 minutes of hold time. The “Cold Pak” exhibits less than 10 degree temperature rise over ambient on full discharge compared to the average of 50 degree temperature rise of all other chemistries. This Cold Pak design dramatically enhances and extends the life of the batteries and the internal UPS circuitry.

The module can be configured via the RJ45 Ethernet network connection to send out SNMP messages indicating overall status of the system to any IP addressable device or queried via a web browser serving up a web page presenting all relevant status conditions of the UPS.

**Power Management – SNMP Status Reporting:** PowerGrid is equipped with an ethernet based Simple Network Management Protocol (SNMP) module for the electronic monitoring of UPS status.
SPUDSTM provides a field deployable capability to monitor and protect Industrial Control Systems (ICS) against anomalous and/or malicious activity both cyber and non-cyber.

**Demand Description**

The electric power industry is losing ground on cybersecurity threats despite the evolution of new cybersecurity standards. As the deployment of digital devices continue to increase, the introduction of new cyber-attack vectors will increase as well. Without the requisite improvements in a control system defensive model, deployments of smart meters and synchrophasors will increase the risk of disruptions and potential loss of administrative control over grid devices. There are three (3) major problems with the lack of defensive capabilities for industrial control systems (ICS):

- Industry has not developed many defensive capabilities for ICS
- Majority of capabilities only protect at the management level of an ICS (i.e. Operator Console or Human Machine Interface)
- Most available capabilities are signature based

**Offering Description**

SPUDSTM is made up of both software and distributed hardware components specifically designed for the detection of insider threats, anomalous and malicious code detection, quarantine and mitigation on the network, continuous network monitoring, message and command level filtering on control system protocols, and helps leverage a multiple defensive vector approach. This greatly increases the capabilities of asset owners to comply with North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards and offers a Defense in Depth approach specifically for control systems.

**Software**

The traffic is collected by a sensor from a network tap where the algorithm breaks the traffic (signal) into lower-level signal components that have unique signatures. By extracting local information regarding the signal in time and frequency domains, malicious attacks may be detected using the changes in data characteristics.

**Hardware**

The SPUDSTM hardware consists of a server operating as the master controller and SPUDSTM database, as well as specialized single board computers operating as the platform.

The SPUDSTM master controller provides a centralized repository for event logging, data correlation and archiving. It provides command and control functions and offers increased situational awareness of their automation environment. The SPUDSTM sensors are deployed throughout the ICS network and operate in a distributed architecture monitoring the network.
SecureEnvironment Product Overviews

• **Environmental Decision Support Suite (EDSS™)**
  - Decision Support Utility for Accessing Environmental Data

• **MOREPower™**
  - Optimizing Siting of Renewable Energy Sources

• **Energy Decision Integration Platform (EDIP™)**
  - Streamlining Regulatory and Operations for Energy Alternatives
EDSS™ is a web application providing an efficient process to aggregate environmental, climate and weather data from various sources into intuitive displays easily manipulated by end users. The web based technology ensures information is accessible from numerous locations and devices, including smart phones and tablet computers.

Demand Description
A common theme when it comes to accessing energy, climate and environmental data sets is that it can be difficult to answer the five basic questions: Who, What, When, Where, and Why. Sometimes even the act of locating a data set or determining how it was generated can prove difficult. It is even more challenging for non-scientific individuals such as planners and policy makers who need to access and include such information in their work.

Offering Description
EDSS™ provides an end-to-end framework for development and visualization of environmental impact and energy products to deliver actionable information for planners and decision-makers in the areas of water resources, traditional and renewable energy planning, public health, infrastructure, and agriculture.

EDSS™ integrates open source packages to create a simple yet robust web application for conglomerating, searching, viewing, and downloading environmental information for both scientists and decision makers alike.

- The Geoportal web application provides an intuitive interface for searching and managing metadata ingested from data sets/data sources.
- The GeoServer and ncWMS web applications provide overlays and information for visual presentations of the data through web mapping services (WMS) by ingesting ESRI shapefiles, NetCDF, and HDF files. Users of the EDSS™ can browse the catalog of available products, enter a simple search string, or even constrain searches by temporal and spatial extents.

Combined with a custom visualization web application, the EDSS™ provides a simple yet efficient means for users to not only access and manipulate climate and environmental data, but also trace the data source and the analytical methods used in the final decision aids products.

While the main goal of EDSS™ is to provide a robust set of tools for decision makers, it can be applied anywhere to rapidly create and display data products to end users.
MOREPower™ allows optimal placement of wind and solar installations to maximize high quality power. MOREPower™ is a paradigm shift for integrating renewable energy into electric grids.

**Demand Description**
Timely, accurate and reliable tools for evaluating, locating, and managing renewable energy resources are critical for maximizing efficiency and ensuring the growth of renewable energy businesses. With new renewable energy markets in India, the U.K., China, Eastern Europe, South America, South Africa, and all corners of the globe, the need for integrated solutions providing web accessible and interactive services that support what-if analyses, big data analytics, and new product creation by the end user becomes more important.

As the US government’s objective is to grow the renewable energy market from 12% to well over 20% by 2030, two key challenges exist: enabling system-level approaches to overall generation capacity extension and integration (including policy changes); and addressing the variability issues of renewable generation.

**Offering Description**
MOREPower™ utilizes High Performance Computing (HPC), proprietary (patent pending) optimization algorithms, and long term resource data sets to evaluate and optimize renewable resource sites more broadly, faster, and with greater precision than existing alternatives.

MOREPower™ quantifies placement of wind and/or solar sites to maximize high quality and complementary power and to drive down risks associated with variability.

MOREPower™ provides:
- Optimal site selection to minimize resource variability, reducing integration costs and curtailment
- Sites evaluation based not just on their expected capacity factor but also on their expected aggregate variability
- Long term wind/solar datasets (15 years) to address variability on a seasonal and inter-annual scale
- Flexible software for inclusion of customer-specific performance metrics.

Furthermore, MOREPower™ quantifies real value of transmission as an enabler to aggregate diverse variable resources. It identifies benefits of larger balancing areas as a key enabler for greater grid stability and therefore a reduced need to keep transmission capacity in reserve. Finally, MOREPower™ provides solutions tailored to reducing price volatility due to intermittency.
Energy Decision Integration Platform (EDIP™)

Streamlining Sustainability Investment Decisions

EDIP™ employs standards-based integration of models and simulations, simulation data management, and data presentation to create an enterprise energy and sustainability decision support system.

Demand Description
In the current environment of cost cutting and green regulations, planners require actionable forecast data for prospective sustainability investments. Decision information with the following qualities is required:

1. Actionable with respect to an organization’s key performance criteria and criteria weights
2. Includes financial, environmental, public perception, and risk considerations
3. Provides the capability to overlay, compare, and contrast forecast results data for candidate projects
4. Shows the impact of prospective investments on organizational, legislative, and Executive Order goals

Offering Description
Northrop Grumman’s EDIP™ is a web-based decision environment for analyzing energy investment and behavior alternatives for meeting organizational energy and sustainability goals. EDIP™ helps decision makers procure and maintain energy consuming systems at the lowest cost while maintaining the highest reliability and efficiency possible for ongoing operations.

EDIP™ simulates alternatives for conservation, behavior modification, renewable energy adoption, alternative energy systems, and conventional systems. The simulation-based alternative analyses predict cost, payback, efficiency increases, emissions reductions, and social impacts while overlaying analyses results with weighted organizational key performance criteria. The system can overlay, compare, and contrast several to hundreds-of-thousands of prospective projects.

System strengths include ease of data capture, web-based system access, and system configurability. Model data is automatically captured by the system without any user burden for data extraction, transformation, and load. The system can be securely accessed using only a web browser. The system views and key decision parameters are configurable. For example, weights for project payback, emissions reduction, and other model predictions can be configured to match organizational preferences.

This system is different because it aids in deciding “what to do from here” and how to do it. By contrast, other systems collect energy and sustainability data but do not focus on decision aids for moving forward. This system offers workflow and life-cycle considerations for managing prospective project decision data and it offers triple bottom line project analysis views. Triple bottom line analyses include Financial, Environmental, and Public Perception considerations.
SecureHealth Product Overviews

• **Enterprise Environmental, Safety & Occupational Health (ESOH)**
  - Leading Solutions for Enterprise ESOH Risk Management and Sustainability

• **PROMIS**
  - PEPFAR Records and Organization Management Information System

• **Public Health Threat Vectors (PHTV)**
  - Actionable Public Health Information
Enterprise Environmental, Safety & Occupational Health (EESOH)

Leading Solutions for Enterprise ESOH Risk Management and Sustainability

EESOH meets the commercial and government need for managing sustainability goals and risk management. For most organizations, facing these challenges is not an optional task, there are serious consequences of not complying with regulatory enforced rules.

**Demand Description**
On top of compliance issues, organizations big and small must manage volumes of data associated with sustainability and EESOH compliance, which include tracking chemical usage, hazardous waste, injury/illness incidents, greenhouse gas emissions, and workers compensation claims.

In the past, most organizations had to either manually record or use various spreadsheets, databases or homegrown applications to track and manage EESOH data and compliance activities. This process can cost organizations from tens of thousands up to millions in manpower and money.

**Offering Description**
The EESOH system provides an integrated solution for managing your organization’s sustainability challenges and EESOH risk management issues.

**Chemical Tracking Module**
Offers a transactional-based process to sustain greening initiatives through product substitution. Allows control of chemical purchases, minimizes waste generation, and supports auditable tracking of material throughout the enterprise.

**Hazardous Waste Tracking Module**
Helps to assure all waste containers are accurately tracked and reported while reducing time and costs to comply.

**Air Management Module**
Provides a powerful engine that allows any organization the ability to calculate pollutant and greenhouse gas (GHG) emissions across an enterprise by scope.

**Industrial Hygiene Module**
Provides the ability for any organization to track employees and identify, evaluate, and control their exposures to chemicals as well as biological, physical, and ergonomic hazards in the workplace.

**What sets EESOH apart from the competition?**
- A process-centric approach configurable to manage all your business processes
- Easy to use and maintain on any network
- Accessible anywhere at anytime
- Flexible technology adapting to existing IT infrastructure
- Integrated management reporting
- Metric performance measurement
- A strong customer base including customers from the Department of Defense, federal government, and Fortune 100 Companies
PROMIS facilitates management of public health indicator & expenditure performance data for HIV/AIDS prevention, care, treatment & health system strengthening services.

**Demand Description**

Reporting of performance indicators is a critical component of global HIV/AIDS intervention activities. Those programs funded by the U.S. government’s President’s Emergency Plan for AIDS Relief (PEPFAR) have Congressionally-mandated reporting requirements. Without an efficient reporting system, this requirement can be difficult to manage and result in staff burn-out when coordinating across multiple Implementing Partners and Agencies.

**Offering Description**

PROMIS (PEPFAR Records and Organization Management Information System) is a secure cloud-based health data system which Northrop Grumman successfully deployed in 2010. PROMIS’ data governance model is based on a shared cloud computing environment.

Currently in use in 10 PEPFAR countries, PROMIS improves public health performance reporting & analysis, better utilizes available resources (especially during reporting cycles), and provides a data warehouse capability to support growing information integration needs.

Prior to PROMIS, results were collected from Partners via templates and manually transferred to master spreadsheets. Partners were unable to analyze or re-use their own entered results. With PROMIS, shared data use now supports Evidence-Based Decision-Making, and improves inter-Agency and partner collaboration. This tool facilitates improvements in multi-agency access to information for planning, budgeting, and program review.

- Supports capture, de-duplication, analysis coordination & reporting of public health indicator & expenditure results across multiple Federal Implementing Agencies, U.S. Country Teams & in-Country Implementing Partners
- Enhances both Program & Country Team productivity & access to quality performance data
- Will expand to support over 30 PEPFAR Countries in 2014

**Extending Lessons Learned to Meet your Needs**

Pulling from our PROMIS experience, Northrop Grumman stands ready to work with national, local, and commercial customers to solve complex records and organization management issues.
PHTV provides the end user with actionable public health information and offers the capability for data manipulation, display and analytics within a self-contained geo-spatial web application.

Demand Description
According to the World Heath Organization (WHO) climate change is a significant and emerging threat to public health, and changes the way we must look at protecting vulnerable populations. Rising average temperatures, in combination with changing rainfall patterns and humidity levels, alter the lifecycle and regional distribution of certain disease-carrying vectors, such as mosquitoes, ticks and rodents. In addition, higher surface temperatures will bring heat waves and heat stress to urban regions worldwide and will likely increase heat-related health risks. Therefore, climate adaptation and health decision aids are urgently needed by city planners and health officials to determine high risk areas, evaluate vulnerable populations, and develop public health infrastructure and surveillance systems.

Offering Description
To address current deficiencies in local planning and decision making with respect to regional climate change and its effect on human health, Northrop Grumman has developed public health decision aids to translate the regional climate and environmental data into actionable information for users. Our methodology involves integrating weather, climate, environmental, demographic, and socioeconomic data sets to quantify the risk of occurrence of vector-borne diseases and heat stress related illnesses.

PHTV products are displayed in a web-based environment, which allows analysts to query, visualize and manipulate public health related information.

Products include but are not limited to:
• Waterborne Diseases
• Heat Stress
• Vector-borne Diseases
• Rodent-borne Diseases

PHTV provides a capability for a better understanding, characterization, and forecast of the anticipated impacts of climate change on public health.

Furthermore, with increasing concerns about the global spreading of infectious diseases, efficient monitoring and surveillance of public health records is critical. PHTV can be used for bio-surveillance, infectious disease hot spots identification and tracking, and statistical analysis of the underlying health data and records.
SecureData Product Overviews

- **DataIMSTM**
  - Information, Management, and Storage Solution for Big Data

- **GeoHome**
  - Extensible Framework for Geospatial Apps

- **AppsEnableTM**
  - Data Processing & Analysis Workflows for Simplified App Creation

- **Paradigm**
  - Big Data Intelligence Harvesting, Exploitation and Analysis

- **Agile ClientTM**
  - Integrated, Lightweight, and Versatile SA and C2 Client

- **RePLACE**
  - Reconfigurable Processor for Legacy Applications Code Execution
DataIMS™ provides customers with information management and storage solutions for Big Data.

**Demand Description**
A wide array of sensors and sources are providing ever-increasing volumes of data. These voluminous data sets are beneficial to many users for a multitude of applications. Data managers contending with the continuous deluge of large data volumes every day are challenged to make the data available to the ever increasing constituency. Users want direct and transparent access to only the data in their specific areas of interest. The demand in our expanding digital world is for information management and storage systems with open architectures to serve data through interfaces with web services.

**Offering Description**
Northrop Grumman designed, engineered, deployed, and operates DataIMS™ as one of the Intelligence Community’s largest information management & storage (IM&S) systems. Our customers are interested in the ease of storing and retrieving Big Data on demand. DataIMS™ handles Big Data. The large-scale distributed storage is scalable to over 20 PB. DataIMS™ uses a hybrid architecture to store over 100 unique data types of unstructured, semi-structured, and structured data in either a file system or a massively parallel relational database. Enterprise-wide solutions are enabled by federated access to external data stores using common data models and ontologies.

The DataIMS™ architecture is scalable in storage size, number of database instances, number of geographic nodes, number of incoming data streams, and number of users. The system boasts world-class ingest rates of 250,000 objects per second per data stream and is capable of handing tens of terabytes of data per day per site. Metadata creation, security labeling, and subscription and notification are handled coincident with ingest, access and management.

DataIMS™ provides users with uniform query and retrieval mechanisms across disparate data sources and geographic locations. We provide our customers with highly selective data retrievals used to uncover “nuggets” via novel search, visualization, and data manipulation. The system has the capacity to service over 1000 queries per hour from 100s of simultaneous users.

Knowing how important your data is to you, DataIMS™ includes information assurance provisions to foster data sharing across the enterprise.

And when it is time to retrieve the data you want, DataIMS™ provides enterprise interoperability with service-oriented constructs and web services for streamlined data exchange.
GeoHome combines a web-service store with frameworks for discovering, building, sharing, and utilizing apps and data across a range of devices.

**Demand Description**
User communities are increasingly using smartphones, tablets and associated app stores. Downloadable apps are a popular approach to provide simple, intuitive tools. Apps respond to consumer demand for timely, customizable and responsive information and tools. Unfortunately, the backbone to exploit developing technologies has lagged behind a platform for developing, posting, and accessing geospatial apps.

**Offering Description**
GeoHome is Northrop Grumman’s platform for developing, posting, and accessing geospatial apps.

GeoHome can support customers with configurations for both web and mobile clients. The web configuration uses Adobe Flex and HTML5 and the mobile configuration uses Android. GeoHome’s underlying framework provides open, extensible, plug-and-play Application Programming Interfaces (APIs) for rapid development of modular and reusable apps to take advantage of shared spatial visualization and analysis capabilities. The GeoHome API enables app developers to write a single app interface to use on both web and mobile clients.

For missions and related applications, finding the right data and services is critical. The GeoHome app-based framework enables users to find the right app to use with available data and services. Discovering the right data is often difficult, as environmental data comes in a variety of formats, resolutions, and coordinate reference systems. GeoHome includes a search engine for geospatial metadata using a graphical user search interface linked to a Representational State Transfer (REST) web service API. Using the web service query approach, a federated search can be set up to query multiple repositories, such as Open Geospatial Consortium Catalog Service for the Web (OGC CSW) catalogs, using a single interface and the available data can be consumed by various apps. Once web services and underlying data are discovered, they can be dynamically integrated with the map for display, or with an analysis app for processing and information extraction. GeoHome users can bookmark desired areas of interest and receive text message or email alerts when new data is discovered or updated for an area of interest.

One of the primary goals of GeoHome is to make data and service discovery, access, and usage by apps seamless and transparent.

The GeoHome framework supports app chaining. App chaining allows the output from one app to be used as input to another app. This enables automating and simplifying advanced processes.

We have an existing family of apps for analysis, data access, search, and other utilities. These apps are available within the GeoHome app store and can be tailored for mission-specific needs.

The power of GeoHome increases as the community adoption becomes more widespread and additional apps are developed by various members of the community.
AppsEnable™ allows customers to chain multiple web services together to simplify the creation of apps.

**Demand Description**

There are many web service apps in use for a wide array of functions and utilities. People are finding ways to chain apps together to enable higher order functions. Knowing the sequences of chaining that work is important for ensuring quality functions and results. Documenting the workflows of all chained apps is essential for maintaining configuration control for key processes used in operational environments. Customers find value in easy to use tools for workflow management.

**Offering Description**

Northrop Grumman’s AppsEnable™ allows developers and users to chain web service apps together to form new workflows on the fly. AppsEnable™ automatically exports the chained services as new apps.

This innovative approach provides quicker access to higher order apps across the organization, mitigating delays from waiting for a developer to write code for an entirely new app.

AppsEnable™ provides a graphical interface to connect to WPS instances. The Open Geospatial Consortium (OGC) Web Processing Service (WPS) is a standard, web service and XML-based interface. AppsEnable™ is geared towards geospatial processes and enables developers to discover, describe, execute, and chain processes. Using this tool, WPS process execution requests can be serialized, saved, and loaded.

The AppsEnable™ interface includes 3 primary components:

- **Process Panel** – connects to multiple WPS instances. Users can click on or drag and drop a process to add it to the diagram/canvas.
- **Diagram/Canvas** – provides a visual representation of a process chain. Users can click on an output in order to connect it to a compatible input.
- **Property Panel** – displays inputs and outputs for the process currently selected by the user. Users can enter text, map data, or files as input. Users can serialize process requests and preview workflow results.

AppsEnable™ provides capabilities for serializing and executing models, clearing the diagram/canvas, saving/loading a workflow/process chain, and automatically arranging a workflow on the canvas. Any process in a workflow can be executed at any time, allowing the user to see intermediate results.

AppsEnable™ can export new process chains as a stand-alone app, a GeoHome app, or a customized app format export interface.
Paradigm is a big data collection, processing and analysis framework for exploiting text, audio and video.

**Demand Description**

The explosion of data in both open source and private source data requires constant innovation in analytic methodology to keep up with the expanding volume. The rapidly changing data within social media, blogs, chat, audio and video need to be combined to determine trends, upcoming threats, potential threats, and events. Mission understanding and applied intelligence tradecraft is required to combine full site, targeted, and smart collection techniques to feed analysis services.

**Offering Description**

Integrating smart and targeted collection techniques and analysis services like alerting, sentiment and temporal analysis into our workflows, moves us one step closer to predicting future events. Paradigm’s architecture contains five major components:

- **Collection** – The gathering of data such as intelligence reports, open source news, user generated data, YouTube videos, Podcasts and Twitter feeds.
- **Ingestion** – Converts any text portion of data into a standards based format for metadata and language identification, and processing.
- **Storage** - Stores the data in an appropriate data repository such as HBase, MySQL, or a File system structure based on the data type.
- **Analysis** – Performs analytics on the data such as entity extraction, geo tagging, relationship identification.
- **Services** – Exposes the results of the analytics and user requested analytics to a user interface or other processing system through standard web services.

**Big Data Analysis**

Northrop Grumman provides automated and user driven analytics in a collaborative, multi-int environment, creating valuable intelligence from massive and ever growing diverse data sources. Paradigm applies multi-media big data search and analysis tools to unstructured text, video and audio data, including:

- **Concept extraction** – popular parts of speech associated with an entity in a given data set or search results.
- **Geospatial tagging** - latitude/longitude, confidence and features from all locations discussed within unstructured text.
- **Integrate multiple search engine types** - combines text, audio, geospatial and image search engines.
- **Alerts based on user defined profiles** - profiles can be on an area of interest, keywords, phrases within audio data, or entity actions.
- **Insights using temporal relationships** – examine historical data to reveal relevant intel/relationships when compared with current/new data.
- **Automated analytics** - examine trends, hot topics, and prediction.
- **Finding and visualizing relationships** - Common interface regardless of the media being searched and analyzed, bringing together a best of breed mix of open source and COTS software to provide an enterprise-level data analytics system.
Agile Client™ is a Northrop Grumman visualization tool enabling customers at different locations to collaborate and see a common operating picture (COP) to accomplish their respective Command and Control (C2) missions.

Demand Description
Emergency responders, city officials, energy managers, logisticians, security officers, and police commanders all need a common view of a situation to effectively conduct their respective missions, while having information on the parallel activities of others operating in the same space.

Offering Description
Agile Client™ is a visualization software package providing situational awareness to the client using a Java-based three-dimensional cartographic modeling engine. The visualization suite is ready to deploy to support users with applications ranging from disaster relief activity to security response. Agile Client™ presents users with 3D views of geo-referenced data as the foundation for a COP. The tool suite includes data management of distributed sources, support for operations decoupled from the network, and the ability to connect to multiple servers.

Agile Client™ has an extensible framework and provides:
- Dynamic configuration of enterprise-wide data
- Terabytes of map data accessible from Web Map Services (WMS) providers
- Weather data from the US National Oceanic and Atmospheric Administration (NOAA) servers
- Commercial FAA data from standard KML feeds
- Current news uploaded from Geo RSS data feeds
- Key web-services using Representational State Transfer (REST) and Simple Object Access Protocol (SOAP)
- Enterprise chat capabilities
- Coordinate across systems
- Collaborative overlays and freehand drawing
- Talk and Voice: instant messaging with VoIP
- Uses open standards compatible with Facebook, Google Talk, and Defense Connect Online, including XMPP and XML streaming protocols
**Demand Description**

Overcoming parts obsolescence and growth limitations of legacy systems is a significant challenge in today's budget environment. When upgrading a processor, the major cost and risk is software, not the new hardware.

**Offering Description**

RePLACE software provides a virtual machine (VM) environment that faithfully emulates the operation of the legacy processor and enables the legacy software binary executables to run on the new processor exactly as it did on the legacy processor. RePLACE allows new software functions to take advantage of the new processor's increased memory and processing speed to be integrated with the legacy software. With RePLACE, a system can gain all of the benefits of modern computing technology while leveraging the maturity and investment that has accrued in the legacy software.

RePLACE virtualization technology offers a cost effective means of achieving significant sustainment and performance improvements through the introduction of modern computer technology in vital systems. It maintains backward compatibility with existing legacy software while providing rapid migration to state-of-the-art processors and software technology. This produces significant cost savings, offers substantial risk reduction, and promotes incremental upgrade opportunities for future enhancements. Also, RePLACE requires no custom hardware – it is embedded software technology that leverages the latest in commercial-off-the-shelf processor technology.

The benefits of applying RePLACE to legacy processor upgrades are threefold:

1. Enormous cost savings are achieved by reusing the existing mission software from the legacy processor. These cost savings are realized by eliminating both software development (true software reuse) and software revalidation costs.
2. Schedules are significantly shortened for completing the upgrades.
3. Performance is dramatically improved in both execution speed and available processing and memory resources.

Although RePLACE was conceived for on-board avionics computer replacement strategies, it is equally effective in other embedded computer applications, such as Command and Control (C2) systems, automated test equipment, weapon system trainers, and integrated support environments.

RePLACE establishes the foundation for hardware upgrades working with trusted legacy software, creating a solid base on which additional software and hardware capabilities can be incrementally added. Powerful support tools provide visibility into the legacy software and facilitate troubleshooting or adding new features, whether the features consist of minor modifications, or the addition of a major new capability.