LEADING THE WAY IN OPEN, INTEROPERABLE ENTERPRISE SOLUTIONS FOR EMERGENCY OPERATIONS CENTERS (EOCs): THE INTERGRAPH'S APPROACH

A. Fiduccia [a, *], R. Di Pace [b]

[a] Intergraph Italia LLC, via Sante Bargellini 4, 00157 Rome Italy – andrea.fiduccia@intergraph.com
[b] Intergraph Italia LLC, via Sante Bargellini 4, 00157 Rome Italy – roberto.dipace@intergraph.com

KEY WORDS: Decision Support, Interoperability, Monitoring, Multisensor, On-line, Standards, Web based

ABSTRACT:

An Emergency Operations Center (EOC) enhances an area's ability to coordinate multi-agency responses to disasters and emergencies.
An EOC is equipped to perform a number of crisis management functions but is also able to function as a day-to-day operations resource and support efforts to test and exercise contingency and response plans. It is activated during an emergency that has overwhelmed the normal day-to-day functions of first responders. It typically performs the following functions: information collection, information processing, information display, information dissemination, management and coordination of interagency activities, implementation of relevant plans and command and control of assigned resources. Generally, an EOC includes communications links (i.e. telephones, two-way radios, patching equipment); computer equipment; map displays to show geographic attributes; dynamic data of the unfolding situation; static reference data; and response plans. This paper presents typical EOC requirements and the technology available to address them.
Whether it's spanning multiple, geographically dispersed sites or crossing jurisdictions and national and local agencies, the ability to share information seamlessly is becoming more and more critical. While many tools and sensors exist to view operational and tactical information, what has been lacking is the ability to tie information from these many systems into a single view that can be shared among disparate organizations. The chief requirement to achieving this is open, enterprise level solutions that can interoperate with many systems, data sources, sensors and technologies.
Intergraph provides the world's leading public safety dispatch system, which is accessed by more than half a billion people worldwide when they dial for emergency response. Because coordination with public safety agencies during a large-scale event is so critical, Intergraph's Computer-Aided Dispatch (I/CAD) system forms the basis for interagency coordination and management of operations and serves as the foundation of the decision support process. I/CAD seamlessly integrates an interactive, real-time map display with call handling, dispatching, records and information management, remote and field access, analysis and models. Intergraph's systems meet IT security requirements – such as the Defense Information Assurance Certification and Accreditation Program (DIACAP) – and dispatch interoperability (APCO, CAP) without compromising performance. Built on standard interfaces, Intergraph products I/Sight, I/Sensor and I/Alarm Plus allow two-way communication with a variety of video, sensor and alarm types.
At the same time, Intergraph has enjoyed a long, successful partnership with the OGC, since its founding in 1994, to create open and extensible software application programming interfaces for geographic information systems (GIS) and other mainstream technologies.
Intergraph offers a broad range of solutions for EOCs. The key to Intergraph's approach is standards and interoperability. The partnerships with vendors, government and military agencies and commercial organizations enables Intergraph to continuously create and hone open and extensible software applications to meet the needs of EOCs.

1. THEORY OF EOC AND REQUIREMENTS

1.1 Introduction

Disasters like Hurricane Katrina and Rita and other have raised critical technological requirements for EOCs. There are many challenges that prevent EOCs from obtaining and sharing the information required to respond effectively to incidents. Perhaps the biggest challenge is interoperability between the multiple agencies involved. Police, fire, public works, health services, emergency medical services and more others they have their own systems and procedures, with data arriving from many sources in all types of formats. EOCs need technology and tools that provide them with real-time collaboration, external data fusion, situational awareness, financial tracking, status reporting and resource and consequence management.

1.2 Standardization and Interoperability

According to U.S. Department of Homeland Security (DHS) interoperability takes on two distinct forms. One is organizational and communicative, the other is technological. Obviously these are tied together. Technology enables improved communications, which allows interagency cooperation. By aligning with organizational and technological standards, an EOC solution can improve interagency communication and cooperation. An EOC solution must meet specific standards. EOCs must report using a standard format and meet basic government policy and requirements for regulations.
Through the cooperation with the state of Louisiana, Louisiana State University (LSU), the U.S. Army Warfighter Protection Lab. and Oak Ridge National Laboratory, Department of Homeland Security and NORTHCOM, Intergraph has worked

* Corresponding author.

to develop and package solutions for EOCs that meet these needs.

The Intergraph's EOC solutions align with U.S. standards such as the National Incident Management System (NIMS) and international standards such as the Association of Public Safety Communications (APCO).

In 2002, APCO published its Project 36 standard for mutual management of shared resources between multiple agencies. This standard features the concept of a coordinated response that allows agencies to continue under their procedures and regulations while keeping other agencies informed through data transfers. As a long-time member of APCO, Intergraph contributed to and aligned its products with these standards. Intergraph developed its InterCAD product to provide an XML-based data transfer of event, unit and communications data between agencies. It provides a bridge between a variety of vendor's computer aided dispatch products, as well as incident command software such as Short Message Service (SMS) systems, EOCs and Intelligent Transportation Systems (ITS).

The Intergraph's EOC solution supports the NIMS organizational structure for emergency response (i.e. Command, Operations, Planning, Logistics, Finance and Admin) by addressing the entire incident management life-cycle process (preparation, response, mitigation and recovery).

Intergraph supports EOCs in every step of the workflow from developing contingency plans and building SOPs and checklists to tracking the progress of the response effort and maintaining status reports.

Intergraph is also directly involved in the development and implementation of technical standards in close association with the Open Geospatial Consortium (OGC®) while cooperating with Microsoft, Adobe, Oracle and others.

The partnership is aimed to create open and extensible software application programming interfaces for geographic information systems (GIS) and other mainstream technologies. Intergraph's GeoMedia® GIS technology, which provides flexibility, interoperability, open architecture and adherence to industry standards, is just one example of this collaboration.

1.3 SensorNet

Additionally, Intergraph adheres to critical information security standards such as DoD Information Assurance Certification and Accreditation Program (DIACAP), National Information Assurance Certification and Accreditation Process (NIACAP) and others. Intergraph is presently working with the Oak Ridge National Laboratory (ORNL), the Department of Energy's largest science and energy laboratory, to implement and promote industry-wide information sharing standards for ubiquitous, cost-effective and secure networks for chemical, biological, radiological, nuclear and explosive (CBRNE) sensors and intrusion detection systems. This project will also address the issues of interfacing sensor networks to local and regional emergency centers and personnel.

This SensorNet will form the basis of the U.S. homeland security sensor network. SensorNet is a net-centric approach to integration of sensors, applications, services and data that allows for a plug-and-play environment for integrating sensors. Sensors communicate to a data center (e.g., a 9-1-1 center) through standard Internet protocols such as 811g and SSL. A new IEEE standard (1451) was developed for sensors to plug-and-play into nodes. The data center is built around OGC's Web Feature Service (WFS). In SensorNet, everything is a spatial "feature," including sensor observations and measurements, sensor and node metadata, location, ownership, associations and even alerts. Routine data are archived in WFS, good for data mining and analysis. All features (data) are tagged with owner labels and certificate-based access control is determined by data ownership. Access determined at request time is based on requestor's credentials.

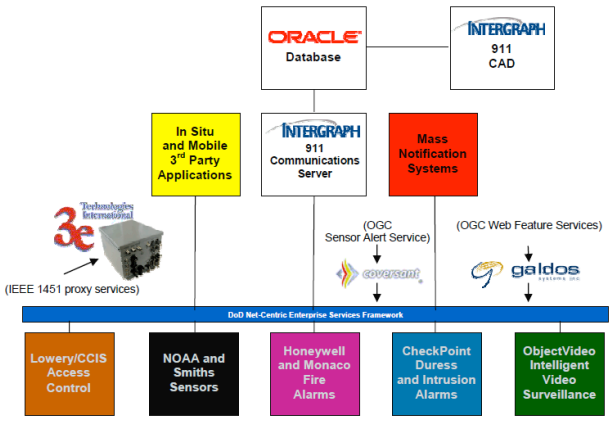

Figure 1. SensorNet Framework

As part of this effort, the ORNL, Intergraph, ObjectVideo and Fort Bragg's Directorate of Emergency Service partnered together to develop and test these standards. They have established a prototype for an Integrated Incident Management Center (I²MC) at Fort Bragg. Insisting on open interfaces, standards and interoperability, ORNL selected Intergraph to provide the foundation of the I2MC solution. The I2MC is a multi-purpose consolidated E9-1-1 system that receives sensor alerts and provides real-time access to comprehensive data from SensorNet. The system also integrates with Fort Bragg's Intelligent Video Surveillance System (IVSS), which automatically tracks and identifies objects that have violated controlled areas, detects a human under variety of ambient lighting conditions and differentiates between human, animal and vehicles.

1.4 Interoperability and Data Sharing

So, an EOC solution must be able to access a variety of data – from utility to transportation to public safety data – since the situational awareness of an EOC is only as good as the data it uses.

Intergraph works closely with Oracle, Microsoft and other database providers to ensure integration and use of multiple data types. In a correct approach to EOC all data (video, audio, telephonic and radio switches, intrusion sensors, infrastructure sensors, perimeter monitoring systems, etc), wherever possible, are accessible throughout the system for authorized users. By fully supporting ITC and GIS standards, Intergraph's solutions can read multiple data types including:

- proprietary geospatial data formats (ESRI, AutoCAD, MicroStation, SmallWorld and others);
- RDBMS "geospatially enabled" (Oracle, MS SQL Server, MS Access, etc);
- OGC's Web Services both cartographic-oriented (WMS, WFS and WCS) and "sensor data streaming"–oriented (Sensor Planning Service, Sensor Observation Service, etc);
- *Mashup* Web GIS technologies (Google and others);
- other sensor data streaming and formats (web services and data servers).

For example, Intergraph's GeoSpatial Monitor (Figure 2) uses advanced spatial information management technology (GeoMedia Data Server) to provide multiple live connections to

more than a hundred GIS, computer aided dispatch (CAD) and image data formats. It then integrates these multiple spatial data formats into a single Common Operational Picture, requiring no translation or re-projection of data.

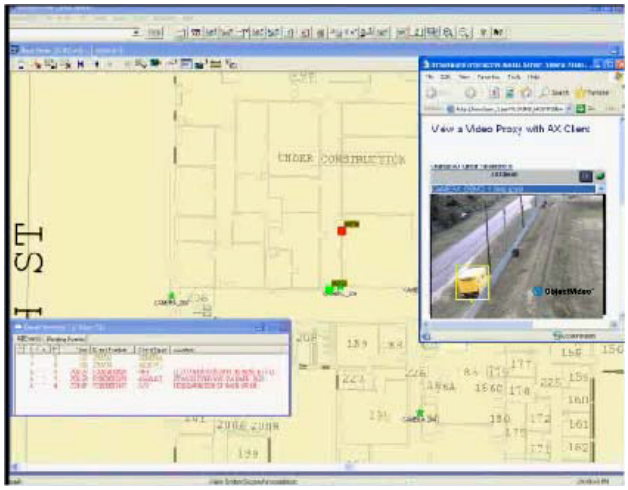

Figure 2. Intergraph's Geospatial Monitor

For the geospatial data infrastructure, as backbone of an EOC, Intergraph's TerraShare® product helps manage and access multiple image and map sources to ensure the use of the latest and most accurate data. It provides transparent access to common imagery using a direct streaming or a WMS, so personnel throughout an EOC or jurisdictional area can use their time more efficiently and make better decisions. This in turn makes response more accurate. Used by LSU for FEMA and the state of Louisiana during Katrina, TerraShare increased situational awareness and helped with the recovery effort.

The design of data sharing policies must consider that data must be put in the correct context and presented in an organized way to be useful to all involved personnel and to the public and considering also that the context may change at each level of decision-making:

- for public is critical a basic map viewing (evacuation routes, road closures, impact areas) and reports (damage assessments, weather forecast, analysis results);
- first responders and dispatchers are more concerned about individual units and capabilities and support of the local mission;
- decision makers require a different context that includes other potentially related events, overall regional capabilities, potential public impact and more.

The same real-time data are needed to populate all displays, which provides a consistent look and feel at each level to reduce the reorientation required for each one. Data at all levels has to be integrated from the incident site to national levels. And it is needed the capability for quickly publishing map, imagery, or analytical data on the Web for internal (intranet) or external (Internet) uses on both desktop and field-computing platforms.

2. PUBLIC SAFETY DISPATCH AS FOUNDATION LAYER OF EOCs

2.1 Basic Computer-Aided Dispatch Features

A public safety dispatch tools often form the basis for interagency coordination and management of operations because coordination with public safety agencies during a large-scale event is critical.

The Intergraph Computer-Aided Dispatch (I/CAD) system is a modular suite of products, designed to be flexible, scalable and provide superior performance in whichever environment it is deployed. Intergraph's "I/CAD customers" vary from Police Forces to Airport security, from Ambulance Services to Border Guards and include sites serving from one to fifty agencies sharing a common system. The same core CAD engine is used for Calltaking, Resource Management and Dispatching: being supremely configurable it allows an agency to develop its own "look and feel", follow their own workflow and use their own terminology.

I/CAD is built on a highly resilient, scalable platform, designed and refined over 20 years of experience in Public Safety, constantly evolving but never losing sight of the vital goal, 100% availability 24 hours a day, 365 days a year. There are a number of possibilities for system architecture.

I/CAD is a networked system with distributed processing, combining both traditional client/server architecture with components of a Service Oriented Architecture. New developments tend to be more service-oriented, but the core client products for call taking and dispatching, are desktop applications, communicating both with the central database and with other components via separate network access methods.

At the centre of the system is the I/Executive product, providing central services and database management tools. This centralises data operations and acts as the core of the highly resilient database infrastructure.

In the Control Centre, the operational tools are I/Calltaker and I/Dispatcher. These two products share a common foundation for taking calls and creating incidents. I/Dispatcher includes the additional functionality necessary for managing resources and interfacing with mobile devices.

In the field, a number of options exist for remote workers. There is a fully featured mobile client including GIS mapping and sophisticated workload management functions. I/Netviewer and I/Netdispatcher extend the CAD desktop to the web, allowing remote workers, teleworkers and management quick access to the system, with incident creation and annotation facilities in I/Netviewer, extended to dispatching in I/Netdispatcher.

Interfaces with external systems are managed by a portfolio of services created from modular components, allowing rapid customisation for different vendors' products. Interfaces generally run on dedicated interface servers, which may be configured in resilient groups with automatic failover. All products use a common resilient database access library, combining industry-standard data access technology from Microsoft with specialised resilience layers from Intergraph, affording a very high standard of data safety.

The I/CAD network Listener completes the picture, providing peer to peer communications between components, keeping the displays synchronised and up to date with every new incident, every new remark, every unit dispatch and minimising database load, allowing great scalability. The listener communicates using a broadcast/acknowledge mechanism, keeping network traffic to a minimum and allowing the deployment of I/CAD across local and wide area networks. This allows the creation of multi-site, regional or national systems, in effect a distributed "virtual control room" where every operator has the ability to manage every incident and resource when required, or to filter the information so that they only see the information for the sector(s) they require, at the click of a button.

Figure 3. Intergraph's I/CAD

2.2 Consequence Management

Consequence management is the process of responding to an event after it has occurred. Intergraph's public safety dispatch system is designed to help EOC personnel respond to non-standard, potentially catastrophic events by executing predefined standard operating procedures (SOPs). With I/CAD, you can define response plans in terms of objectives, strategies and tasks and define a set of objectives for every response plan. This helps to coordinate the response across all levels of an EOC, ensuring that no task is unallocated or forgotten.
I/CAD also enables operators to access major incident response plans and follow the associated National Incident Management System/Incident Command System (NIMS/ICS)-compliant checklists. It limits information overload, however, through the use of pre-defined rules and operational concepts. Intergraph's dispatch solution also logically queues information for operators and recommends a course of action that accounts for factors such as temporal conditions, special events and traffic conditions.

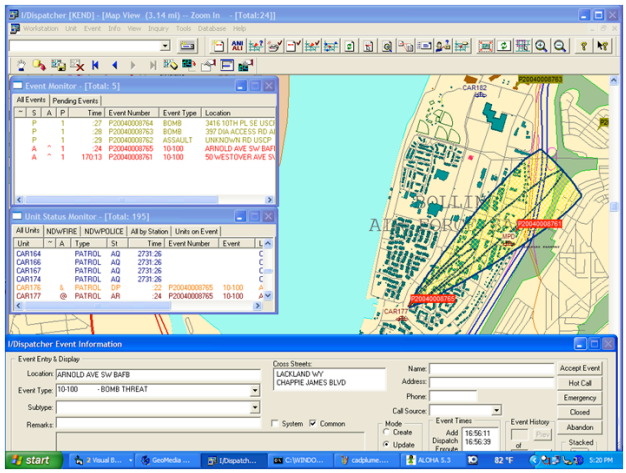

Figure 4. ALOHA integrated with I/Dispatcher

Intergraph's public safety dispatch system also addresses the need to have a real-time asset catalog available during a major incident. This asset catalog dynamically updates recorded assets deriving from manual entry, sensors, external databases, or a combination of all three. Operators can import, input and maintain site-specific asset data; search for assets; manage the quantity, status and location of each; and obtain a real-time, accurate picture of all assets available despite your location.

Intergraph's solutions integrate also tools ranging from the Corps of Engineers (blast modeling) to the DOT (traffic modeling) as well as popular plume modeling tools, such as ALOHA (Figure 4).
Finally, Intergraph is the first computer-aided dispatch (CAD) provider supporting the Unified Incident Command and Decision Support (UICDS) project. UICDS is sponsored by the Science and Technology Directorate of the U.S. Department of Homeland Security and is being executed through a contract with prime contractor Science Applications International Corporation (SAIC). The UICDS project will advance rapid incident response and situational awareness through the creation of a national architecture for emergency information sharing across jurisdictions and applications.

2.3 Incident Command

The incident command structure is a critical component within NIMS to manage an incident and its consequences. Because some EOCs are highly mobile or may require specific management tools, Intergraph has developed an incident command tool. This tool serves as the core of an EOC and provides a lightweight system to view and manage resources and activities associated with an event providing integrated situational awareness during planning, response, recovery and mitigation. Its open architecture and standards-based design provides the interoperability and information sharing vital for success during each phase of consequence management. It also helps prevent uncoordinated planning, shared information lapses, lack of unity of purpose and improper execution of response SOPs.

2.4 Mobile Resource Management and Collaborative Environment (Common Operational Picture)

Mobile Resource Management (MRM) manages real-time location information on assets – such as vehicles, equipment, emergency supplies and more – and monitors them remotely. Intergraph helps alleviate the concerns surrounding mobile resources management by taking an integrated approach. Our MRM solutions (Geospatial Integrator for Onsite Troops and Tracks Observation) go beyond simple resource monitoring to what we call presence management. This Common Operational Picture (COP) console integrates several key components – wireless communications, geospatial software, location tracking tools and the Internet –helping operators to plan, manage and track mobile assets and personnel. Intergraph's Geospatial Integrator for Onsite Troops and Tracks Observation can track and manage multiple resources using the latest in radio frequency identification (RFID) technology, global positioning systems (GPS), automatic vehicle location (AVL) systems, cell and sensor technologies and geospatial mapping applications (2D and 3D COP interfaces).
This solution offers both thick- and thin- client systems to view and manage these resources and a SmartClient (Intergraph's ResPublica Intranet) to establish rules such as zones of operation or set off-limits areas that will create an alarm upon entry. The solution it is designed to become a client of OGC's Web services and to publish maps and reports on the Internet (using GeoMedia WebMap, Intergraph's geospatial Web server).

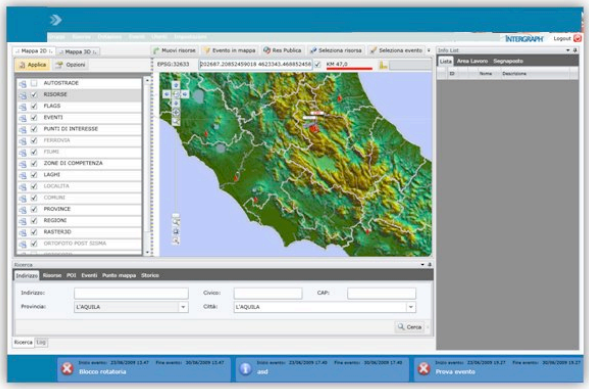

Figure 5. Intergraph's Geospatial Integrator for Onsite Troops and Tracks Observation (2D COP)

Using this solution for EOC, Intergraph, as part of a team led by SELEX Sistemi Integrati (SSI), the systems integrator for the Finmeccanica Group, played a vital role in successfully ensuring the safety and security of world leaders, guests and infrastructure at the G8 Summit, held in L'Aquila, Abruzzo, Italy, from July 8–10, 2009. Intergraph's solution provided a common operational picture that aided Civil Protection Department personnel in their efforts to secure vulnerable areas, detect and assess threats and quickly respond to incidents. The integrated security system also enabled the exchange of intelligence between the Central Management Station and several remote command and control centers.

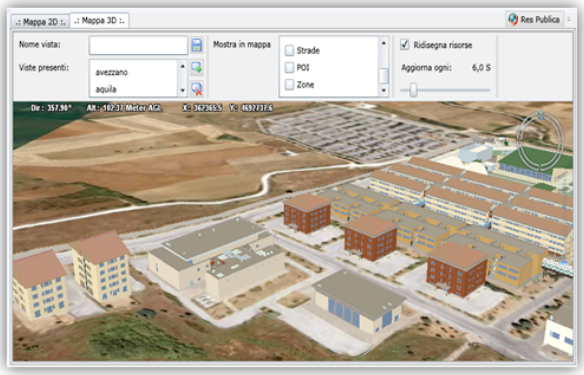

Figure 6. Intergraph's Geospatial Integrator for Onsite Troops and Tracks Observation (3D COP)

3. CONCLUSIONS

As a result of the work within the public safety and national security sectors, with partners ranging from the U.S. Army Corps of Engineers and Department of Energy to vendors such as Cisco, ObjectVideo and Skyline, Intergraph has developed a number of solutions that are leading the way in open, interoperable enterprise solutions for Public Safety & Security and for EOCs. All of Intergraph's products are built on industry-standard, non-proprietary formats and platforms, such as the Common Alerting Protocol (CAP) and Web Features Servers (WFS). This enables the products to be easily ported from one system to another and adapted and developed to meet specific industry requirements and specific SOPs of different countries.

One in 12 people in the world is protected by Intergraph public safety and security solutions.

REFERENCES

Botts, M., Percivall, G., Reed, C., Davidson J., 2007. *OGC® Sensor Web Enablement: Overview And High Level Architecture*, OGC White Paper, pp. 12.

Mérigot, P., 2007. *OpenGIS® Sensor Planning Service Application Profile for EO Sensors*, OpenGIS Discussion Paper, pp. 134.

NGA National Geospatial-Intelligence Agency, 2006. *Geospatial Intelligence Standard – Enabling a Common Vision*, 2006, pp. 20.

US Homeland Security Department, 2008. *National Incident Management System*, pp. 134.

US Homeland Security Department, 2008. *National Response Framework*, pp. 82.

APPENDIX A. PUBLIC SAFETY & SECURITY STANDARDS

Standard (Classification):

- SensorML OGC 05-086 (GIS)
- Sensor Observation Service OGC 05-088 (Sensors/GIS)
- Sensor Web Enablement OGC 05-090 SWE Architecture (Sensors/GIS)
- BSR/CSAA CS-V-01-200x Alarm Verification and Notification (Sensors/Alarms)
- BSR/ASTM Z8363Z-200x Guide for Selection of Security Control Systems – Part 1 Defining the Machine-Environment Interface (Interoperability)
- BSR/NFPA 731-200x Standard for the Installation of Electronic Premises Security Systems (Alarms)
- ANSI INCITS 385-2004 Information Technology – Face Recognition Format for Data Interchange (Interoperability)
- ANSI INCITS 377-2004 Information Technology – Finger Pattern-based Interchange Format (Interoperability)
- BSR/IEEE 1700-200x Security Architecture for Certification and Accreditation of Information (Planning)
- BSR/IEEE 1700-200x Security Architecture for Certification and Accreditation of Information (Planning)
- BSR/NSF 4xx-200x Homeland Security Protection for Food Delivery (Planning)
- BSR/NFPA 1620-200x Recommended Practice for Pre-Incident Planning (Planning)
- 1451.2-1997 Smart Transducer Interface for Sensors and Actuators – Transducer to Microprocessor Communication Protocols and Transducer Electronic Data Sheet (TEDS) Formats (Interoperability)
- ISO 4121:2003 Sensory analysis – Guidelines for the Use of Quantitative Response Scales (Interoperability)
- ISO/IEC 10181-1:1996 Information Technology – Open Systems Interconnection – Security Frameworks for Open Systems: Overview (Interoperability)
- ISO/IEC 10164-7:1992 Information Technology – Open Systems Interconnection – Systems Management: Security Alarm Reporting Function (Interoperability)
- ISO/IEC 10181-2:1996 Information Technology – Open Systems Interconnection – Security Frameworks for Open Systems: Authentication Framework (Interoperability)
- ISO/IEC 10181-3:1996 Information Technology – Open Systems Interconnection – Security Frameworks for Open Systems: Access Control Framework (Interoperability)
- ISO/IEC 10164-8:1993 Information Technology – Open Systems Interconnection - Systems Management: Security Audit Trail Function (Interoperability)
- ISO/IEC 10181-4:1997 Information Technology – Open Systems Interconnection – Security Frameworks for Open

Systems: Non-repudiation Framework – Part 4 (Interoperability)
- ISO/IEC 10181-5:1996 Information Technology – Open Systems Interconnection – Security Frameworks for Open Systems: Confidentiality Framework (Interoperability)
- ISO/IEC 10181-6:1996 Information Technology – Open Systems Interconnection – Security Frameworks for Open Systems: Integrity Framework (Interoperability)
- ISO/IEC 10181-7:1996 Information Technology – Open Systems Interconnection – Security Frameworks for Open Systems: Security Audit and Alarms Framework (Interoperability)
- ISO/IEC 10736:1995 Information Technology - Telecommunications and Information Exchange Between Systems – Transport Layer Security Protocol (Interoperability)
- ISO/IEC 10745:1995 Information Technology – Open Systems Interconnection – Upper Layers Security Model (Interoperability)
- ISO/IEC 11577:1995 Information Technology – Open Systems Interconnection – Network Layer Security Protocol (Interoperability)
- ISO/IEC 11586-1:1996 Information Technology – Open Systems Interconnection – Generic Upper Layers Security: Overview, Models and Notation (Interoperability)
- ISO/IEC 11586-2:1996 Information Technology – Open Systems Interconnection – Generic Upper Layers Security: Security Exchange Service Element (SESE) Service Definition (Interoperability)
- ISO/IEC 11586-3:1996 Information Technology – Open Systems Interconnection – Generic Upper Layers Security: Security Exchange Service Element (SESE) Protocol Specification (Interoperability)
- DO-230A Standards for Airport Security Access Control Systems (Planning)
- NZMP 6653 Information Systems Security Standards Handbook (Planning)
- AS/NZS 4471 Information Technology – Open Systems Interconnection – Network Layer Security Protocol ISO/IEC 11577: 1995 (Interoperability)
- NIST 800-14 Generally Accepted Principles and Practices for Securing Information Technology Systems (Planning)
- TR99.00.02 Integrating Electronic Security into the Manufacturing and Control Systems Environment (Planning)
- TR99.00.01 Security Technologies for Manufacturing and Control Systems (Planning)
- ISO 19117:2005 Geographic information – Portrayal (GIS)
- NFPA 471 Recommended Practice for Responding to Hazardous Materials Incidents, 2002 Edition (Planning)
- NFPA 450 Guide for Emergency Medical Services and Systems, 2004 Edition (Planning)
- NFPA 1561 Standard on Emergency Services Incident Management System, 2002 Edition (Planning)
- NFPA 424 Guide for Airport/Community Emergency Planning, 2002 Edition (Planning)
- AS/NZS 4270.1 Geographic Information Systems – Spatial Data Transfer Standard Part 1: Logical Specifications (GIS)
- AS/NZS 4270.3 Geographic Information Systems – Spatial Data Transfer Standard Part 3: ISO 8211 Encoding (GIS)
- AS/NZS 4270.4 Geographic Information Systems – Spatial Data Transfer Standard Part 4: Topological Vector Profile FIPS PUB 173-1B: 1994 (GIS)
- ENV 13729 Health Informatics – Secure User Identification – Strong Authentication using Microprocessor Cards (Planning)

APPENDIX B. OGC'S STANDARDS ENDORSED BY NATIONAL SYSTEM FOR GEOSPATIAL-INTELLIGENCE (NSG)

"Open Geospatial Consortium (Ogc) Spatial Data Infrastructure (Sdi) 1.0 baseline:
- *Web Features Service (WFS): The WFS implementation specification allows clients to retrieve and update geospatial data encoded in Geography Markup Language (GML) from multiple WFSs. It defines interfaces for data access and manipulation of geographic features, and through these interfaces, a web user or service can combine, use, and manage geo-data.*
- *Web Map Service (WMS): The WMS implementation specification supports the creation and display of registered and super-imposed maplike views (graphical images, such as GIF, JPEG, TIFF, and NITFS).*
- *Web Map Context (WMC): The WMC implementation specification is a companion to WMS. It describes how to save a map view comprised of many different layers from different Web Map Services.*
- *Web Coverage Service (WCS): The WCS specification allows access to geospatial "coverages" (raster data sets) that represent values or properties of geographic locations rather than WMS-generated maps (pictures).*
- *Geography Markup Language (GML): GML is eXtensible Markup Language (XML) encoding for the transport and storage of geographic information, including both the spatial and non-spatial properties of geographic features.*
- *Styled Layer Descriptor (SLD): The SLD standard defines the structure of an XML file that applies rendering or symbolization rules to features. An SLD requests a WMS to present a map according to submitted style rules.*
- *Catalog Services (CS-W): The CS-W provides an abstract model and protocol-specific solutions for the discovery of geospatial resources. Through catalog metadata and query interfaces, metadata properties are returned to the requestor, often embedded with links to actual data or services that allow the catalog to act as a referral service to other information resources.*
- *Filter Encoding Specification (FE): FE is used to express a query or filter using a predicate language, or terms and operators, stored in XML elements. FE is used in requests to WFS and queries to CS-W.*

Additional standards included in the NSG baseline are:
- *ISO 19115 Geographic Information - Metadata: critical to making data discoverable and retrievable.*
- *ISO 19119 Geographic Information - Services: critical to defining where web services are deployed and used within an SOA.*
- *NSG Feature Data Dictionary and NSG Feature Catalog: critical to enabling the development of logical and physical data model*" (NGA, 2006, pp. 4-6).