

The Future Evolution of Multi-Level Security for the Federal Government

Table of Contents

Part 1: Introduction	1
Utilizing real-time collaboration to enhance effective information exchange in a multi-agency situation	
Part 2: The Threat	2
A real life hypothetical facing the United States	
Part 3: The Problem	3
Challenges facing current information assurance practices	
Part 4: The Solution	4
Multi-level security (MLS) collaboration	
Part 5: Ezenia and MLS	5
How Ezenia supports MLS	
Part 6: The Future	7
Future of Ezenia and MLS collaboration	

Part 1: Introduction - Utilizing real-time collaboration to provide effective information exchange in a multi-agency situation

In the first decade of the 21st century extreme events have unfortunately brought to the forefront serious challenges facing our country. Disasters, both man-made and natural, have spotlighted our country's need to operate more efficiently across all levels of government. What has been demonstrated is that no matter the cause of a disaster, the many agencies within federal, state, and local governments have not been able to put the necessary information into the proper hands when the situation calls for open data sharing. All indications, to this point, are that we have not even begun to leverage technology in order to push through the procedural impediments to progress.

This report explores the impact of new requirements for secure information sharing between the classified networks of the defense, intelligence, and homeland security offices and the unclassified networks of state and local governments. It will also highlight the basic capabilities of the Ezenia InfoWorkSpace (IWS) collaboration suite to operate in this Multi-Level Security (MLS) environment, and how it might be adapted to meet specific future requirements.

Part 2: The Threat - A real life hypothetical facing the United States

Intelligence: Chemical attack planned in Washington D.C., Metro station

The [censored] blocks below indicate information removed during transmission by one of the agencies:

One hour ago, at 0800, a credible source was interviewed by [censored] sources in [censored], identifying a terrorist cell in Washington, D.C. The source indicates that a chemical agent has already been successfully infiltrated into the U.S., via Canada, and that the target is the capital. The [censored] identified two intercepts, which can potentially be related. The [censored] has the name for one of four men believed to be in a sleeper cell in our nation's capital. The U.S. Border Patrol raises the flag on two men who crossed the border more than four months ago. The [censored], has forwarded a sketch to the U.S. [censored] community, based on [censored] sources, of what the leader of the terrorist cell looks like. The Washington D.C. Police Department has a picture of the leader but have no reason to escalate or share it with the national effort now underway to protect the capital.

None of this data has been synchronized and the attack is scheduled to take place in twelve hours.

The situation described in Figures 1 and 2 is not unusual. There are stovepipes of information which are compartmentalized based on "Need to Know," security classification, and other cultural and physical walls that have been built over the last thirty years.

The Critical Issue

How do we bridge the security of our networks, and quickly enable federal, state, and local agencies to communicate and collaborate, with different networks and levels of security.

Figure 1 – Both National and Local Organizations have Key Information



Agency	Intercepts	Name of Terrorist	Sketch of Terrorist	Chemicals Detected	Picture of Terrorist	General location of Terrorist
NSA	K	U				
DIA	U	K				
US Border Patrol				K		
Multi-National Forces - Iraq	U		K			
FBI				U	U	U
Washington DC police					K	K

Legend: K = Information Source - Know they have valuable info
U = Information Source - Unaware that info is of value

Figure 2 – Threat Matrix for Ownership of Information

Part 3: The Problem - Challenges Facing the Current Information Assurance Practices

In order to provide proper information assurance generally an agency's IT group stands up a single classification computer network. Should the agency require additional classifications, another "Stovepipe" system would need to be established. This method has proven effective in properly securing the data within a single classification. However it has left communication even within a single organization segmented and inefficient. Most people would be surprised to discover that, not only does the U.S. federal government not have a seamless network for information exchange between agencies, but often wings of the same agency cannot share the necessary data in a timely fashion.

In most people's minds, there is a vision of this interlocked web of government agencies communicating over one secure network, as depicted in Figure 3 below. However, this is far from the case. As described above, most agencies have their own network at the necessary classification levels and a classified network at one agency almost never communicates with a network of the same level at another agency. So, instead of an interlocked web of agencies, it is much more a series of islands with loose bridges patched between them. Throw in the need for the government to bring our coalition partners into the communication grid, and the current situation becomes even worse.

When one starts to imagine adding the state and local networks, which mainly run over the public Internet, the complexities expand exponentially. How does the federal government share information securely, but efficiently with those that are forced to deal with our threats at the onset of a disaster?

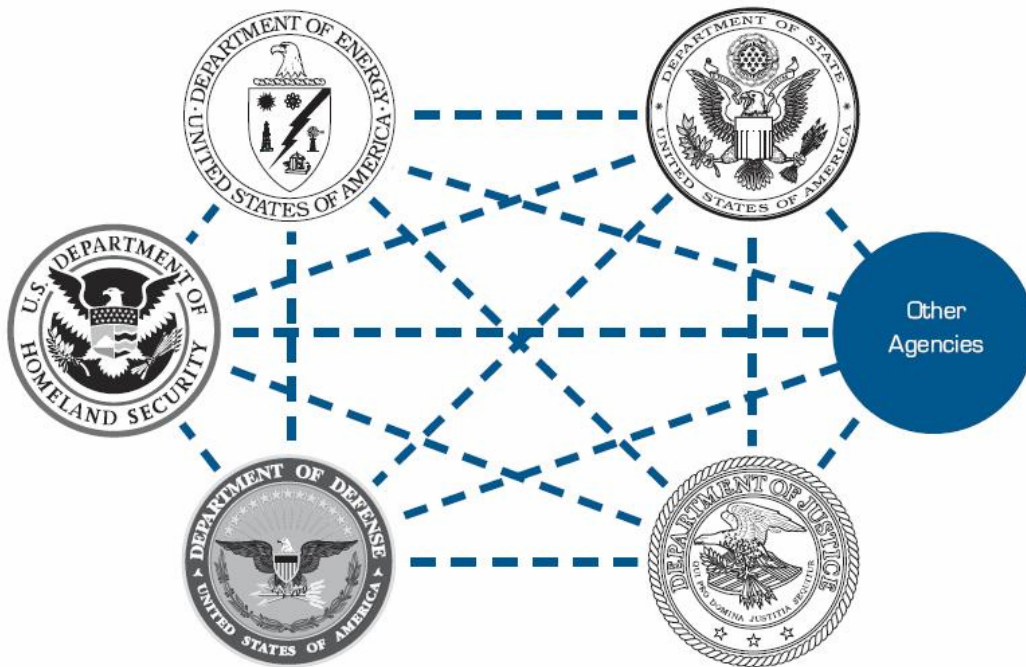


Figure 3 – Current Agency Networks, Same Classification Level

Part 4: The Solution - Multi-Level Security Collaboration

Multi-Level Security (MLS) has been a known challenge to the security community since the 1960s. Despite the efforts implemented by developers, systems have rarely provided the quality of security desired by the most demanding customers in the military services, intelligence organizations, and related agencies. In theory MLS appears to be a simple problem in access control; however in reality the solution is much more complicated.

The foundation of MLS was built to allow information to flow freely between individuals in a computing environment, who have security clearance, while at the same time preventing leaks to unauthorized users. The challenge is how to enforce restrictions with high reliability, and at the same time allow system users and administrators to utilize the tools needed.

The original MLS solution was for two agency's IT groups to stand up a single stovepipe computer system to foster some level of data sharing. Usually, this was a very limited data set, often just file FTP. If additional classifications were required, or information needed to be shared between other agencies or for other missions another "Stovepipe" system would need to be established. This method has proven to be inadequate in today's dynamic environment of an ever growing list of threats and disaster situations.

In today's computing environment, information flows from all corners of the globe from a variety of different agencies and organizations. The value of cross agency MLS has become more critical for the nation's management of sensitive information. Data needs to be cataloged, classified, redirected, and secured at all times, while still being readily accessible to those who need it.

With the continuing threat of global terrorism and severe weather conditions the need for information sharing to facilitate rapid management and response requires MLS deployment within all levels of government agencies. In the past, MLS was focused on data and networking, which remains very important; however, with the use of real-time collaboration, security analysts are developing new requirements. How can MLS collaboration help to foster an environment of information sharing, in contrast to decades of information protection? Somehow the basic functions of collaboration will have to be used for proper information sharing across networks.

Basic Collaboration Functions

The basic collaboration functions required for MLS are:

- **User Profiles** - consist of contact information such as rank, organization, areas of expertise, current assigned projects, and may also include a photograph.
- **Text Chat** - is an instant messaging system that can be used in both virtual meetings and private chat sessions.
- **File Upload** – enables individuals to import remote information into the collaboration environment, by uploading files to their personal directory or into a virtual room filing cabinet. Each file may also have permissions set that restrict access to different teams or individuals.
- **Whiteboard** - Allows images to be imported or created in a shared application, and provides participants with the ability to mark up the document. The edited file can then be stored, retrieved, and recalled at any time.

The MLS Collaboration Mission

The critical mission of MLS collaboration platforms is to:

- Augment the direction of communication and data sharing from the nation's strategic apparatus, through federal agencies, local and state organizations, and down to their associated first responders.
- Provide a cross domain, Multi-Level Security architecture that will make available a time-sensitive, real-time, persistent, and synchronized environment that can be utilized by organizations regardless of their network configurations. "Security zones" should also be created to enable information to transfer from network to network.

Part 5: Ezenia and MLS Collaboration Today

Ezenia has been involved in collaboration within the government since 1997 and provides the tool needed to accomplish these missions.

Figure 4 below depicts how different levels of government could augment the use of existing networks with Ezenia InfoWorkspace (IWS) servers with Security Guards today to protect data classifications

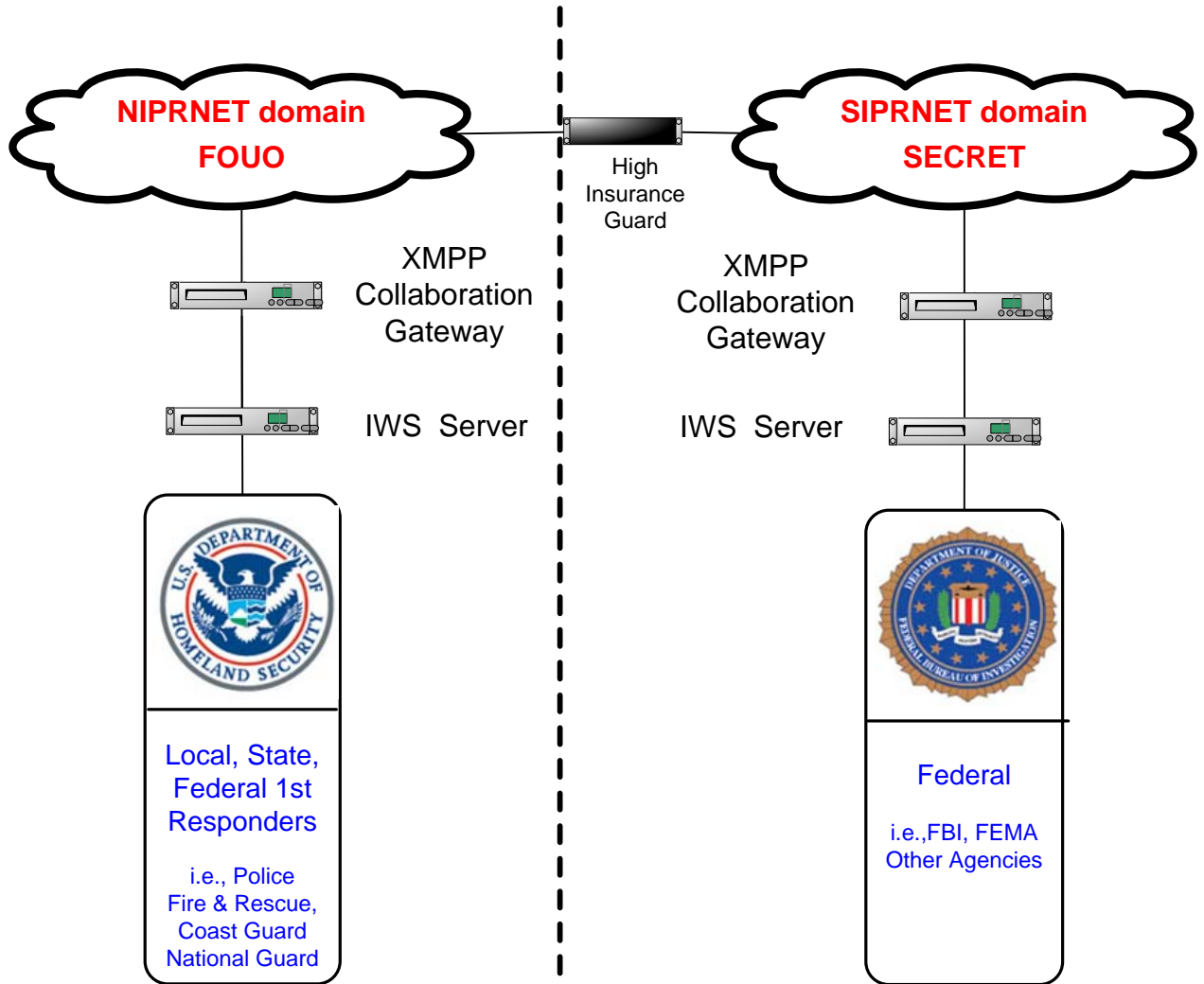


Figure 4 – IWS Cross-Domain Information Sharing Today Using Existing Networks

As depicted in Figure 4 above, High Security Guards and XMPP Collaboration gateways positioned between different domains with different security levels act to filter communication to maintain desired security levels.

IWS 3.0 contains many MLS features supporting effective and secure information sharing. These features are the direct result of requirements and recommendations provided by a variety of government agencies.

IWS provides an environment where users are comfortable sharing data across domains and different levels, while at the same time making sure that the data being shared is secure.

All content and data resident in the system is classified in order to be shared across networks. The security guard depicted in Figure 4 above uses classification as a primary filter applied to information traversing networks.

IWS supports classification by tagging all data being used in an MLS environment. Tagging enables user awareness of all information, windows, and dialog screens being used by users.

Situational awareness is another attribute of user awareness. All IWS screens can be customized both graphically and textually to make it clear to the user which virtual area the user is operating.

User profile tags have been added to help manage both inputs and outputs within the user's knowledge base. Visual prompts were also added to windows and dialogue boxes to indicate to the user their location within the collaboration environment, and what level of clearance they are authorized to perform. The server administrator also has the ability to customize a classification bar with a specific color and title to represent unique levels within the agency.

After applying the proper classification markings and providing the user with the situational awareness necessary, the final aspect of the IWS MLS solution is a robust auditing capability. Event recreation is a key component of any MLS communication. Agencies must have the ability to identify the improper use of secure information should a breach occur. IWS audits all data that can be passed across networks and provides dirty word searching across that audited data to more easily highlight breaches in security.

All of these additions to the software allow IWS to function as part of the bridge between classified networks and allow for efficient and safe information sharing.

MLS collaboration speeds information flow and improves responsiveness

If the agencies described in the scenario at the beginning of this white paper had networks of IWS servers, XMPP collaboration gateways and high insurance gateways similar to Figure 4, the resultant outcome could have taken a much different course as described below:

- NSA and DIA could have used their existing IWS servers to connect the name of a terrorist with his cell phone and general location.
- Via Joint Forces Command and DIA, a copy of the sketch of the terrorist leader could have been identified.
- The detail on the cell phone, general location, and the name of the terrorist leader could have been shared with the FBI. This information would have included the sketch, and allowed key terrorism experts from all agencies to meet in a virtual room and review and discuss the information.
- The FBI contacts the United States Border Patrol and the Washington D.C., Police Department, and within minutes could have had local, state, and federal terrorism offices online using IWS.
- U.S. Border Patrol could then have provided names and pictures of two suspects who were caught bringing chemicals into the U.S. by way of Canada.
- The Department of Homeland Security and the FBI could now have the names of three terrorists and a sketch of the leader.
- The FBI and DHS could have used the High Insurance Guard (HIG) to pass data and information from the National Intelligence Agencies to the Border Patrol and D.C. Police Department. A copy of the sketch would have been populated, in real-time, into IWS and the D.C. Police Department could have immediately recognized the sketch and connected it with an actual photo.
- Within 8 hours, the suspects could have been identified, their location identified, and the area is blocked off as security forces move in to neutralize the suspects.

In summary, the IWS MLS network could have provided a much better outcome for the scenario described at the beginning of this whitepaper. Intelligence agencies, federal agencies, DHS, local and state governments and first responders could have all moved data between organizations, using existing networks, to better manage this crisis situation.

Part 6: The Future - Ezenia and MLS Collaboration

Ezenia sees MLS collaboration as a key component in our government's ability to effectively identify, assess and address security threats today. Ezenia will continue to invest in providing greater capabilities in secure information sharing. Filtering appliances are beginning to appear in the form of High Insurance Guards and as Ezenia continues to refine its information input security tagging they will become more capable, accurate, and effective. Ezenia will continue to enhance its products, to be guard agnostic as depicted in Figure 5 below.

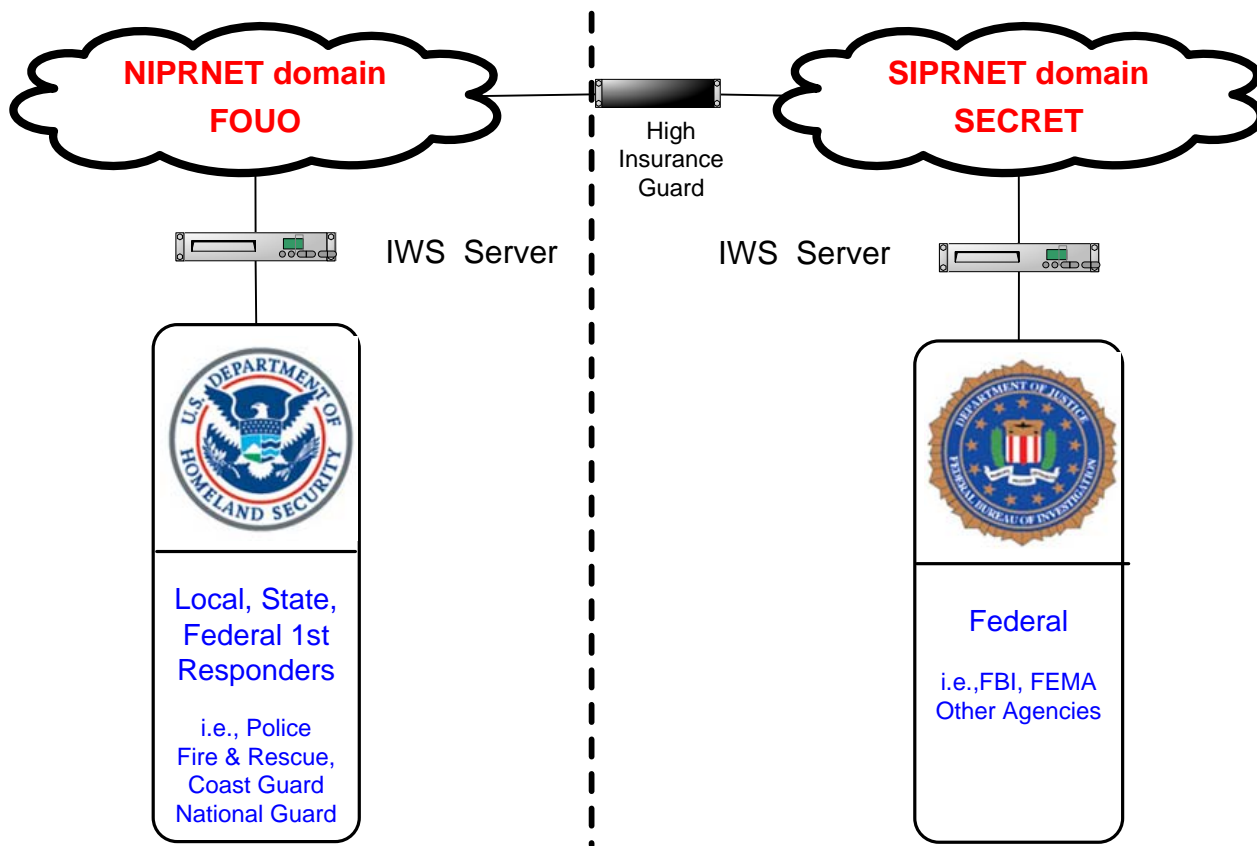


Figure 5 – IWS Cross-Domain Information Sharing in the Future Using Existing Networks

Intelligent algorithms with additional tagging and use of dirty word search software programs are emerging that in conjunction with the IWS MLS solution, can begin to provide real-time capture of security breaches..

While the current MLS solution is primarily text based, with presence, awareness and text chat taking the lead, the need for more media rich applications is obvious. Imagine the ability to share documents, graphics, and whiteboards between two distinct secure networks. Audio and video capabilities are a tremendous potential for improvement in MLS communication. Ezenia will continue to be at the forefront of these efforts to bridge the gap between the agencies that prevent and respond to security threats and disasters.

The future for MLS and collaboration is obvious. The need is now, some capabilities are available, and with proper focus applied to effective, real-world implementations, our government can enhance its ability to provide the security that is expected by its citizens.

For more information visit, www.ezenia.com.

Ezenia Inc. – 14 Celina Avenue, Suite 17 – Nashua, NH 03063 – 800-966-2301

© 2007 Ezenia! Inc. The information contained herein is subject to change without notice. The only warranties for Ezenia products and services are set forth in the contract warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Ezenia shall not be liable for technical or editorial errors or omissions contained herein.

EZ07-1015-v2

