

Multi-Level Security Strategies for the Federal Government

**Harnessing MLS Compliance Requirements
to Improve Agency Operations**

LARSTAN
BUSINESS REPORTS

Copyright © 2004
All rights reserved

Harnessing MLS Compliance Requirements to Improve Agency Operations

Part 1	Executive Summary: Harnessing MLS Compliance Requirements to Improve Agency Operations	3
Part 2	Market Impact Analysis: National Security Requirements in the Post-9/11 Era	5
Part 3	Operational Impact Analysis: Creating a Security Utility	10
Part 4	Security Impact Analysis: MLS Characteristics and Compliance	14
Part 5	Solutions Impact Analysis: IBM's DB2 MLS Meets Common Criteria Standards	19

Editorial Director
Lane F. Cooper

Research Associate
Elliot M. Kass
Elizabeth E. McHugh

This document was developed with IBM funding. Although the document may utilize publicly available material from various vendors, including IBM, it does not necessarily reflect the positions of such vendors on the issues addressed in this document.

Multi-Level Security Strategies

Part 1: Executive Summary

Harnessing MLS Compliance Requirements to Improve Agency Operations

This ***Larstan Business Report*** explores the impact new secure information sharing requirements are having on agencies with defense, intelligence and homeland security missions. It reports on how one company, IBM, is providing platforms for managing these new requirements.

The need to share information among different governmental agencies has risen dramatically due to the war to combat terrorism. Increased emphases on information-sharing among agencies tasked with protecting U.S. national interests at home and abroad have placed greater responsibilities for handling national security information on local and federal agencies that, in the past, have been outside the normal channels of classified information processing.

The traditional approach to enforcing multiple security levels (MSL) has been for each federal agency to operate a separate computing infrastructure for each level of security authorization in force at that agency. A discrete network with one set of servers and storage devices is deployed for top secret data; another is maintained for secret data and yet another for unclassified data (in some cases, all classifications of data are replicated on the servers with the highest security ratings).

This traditional approach, however, is inconsistent with the new mandates to share information to respond to – or prevent – threats to U.S. interests. As a result a better architecture for inter-agency data sharing is being implemented by government agencies: multi-level security or MLS.

MLS has two primary goals.

- First, establish controls that prevent users from accessing information at a higher classification than their authorization permits; and
- Second, ensure that the controls prevent unauthorized users from declassifying information.

Effectively implemented, MLS systems ensure that data can be consolidated onto a single infrastructure, while maintaining the highest levels of assurance that it can only be accessed by authorized users.

According to a joint ***Larstan Business Report/Government Security News*** survey of 214 security professionals working at federal agencies with a national security mandate, respondents overwhelmingly agreed that the war on terror has increased the importance of information security.

- 90 percent of respondents believe the importance of information security is growing because of the war on terror.

Multi-Level Security Strategies

- 74 percent report that the adoption of E-Government initiatives is also elevating the importance of information security among federal agencies tasked with protecting U.S. national interests.
- 65 percent of respondents report that their agencies must adopt MLS strategies in order to protect information that is shared with other agencies.
- 65 percent of respondents indicate that their agencies are currently involved in an infrastructure modernization initiative.
- 47 percent report that MLS initiatives are driving requirements for these infrastructure modernization initiatives.
- As agencies wrestle with how to consolidate and integrate current silos of classified infrastructures, 38 percent report that the mainframe platform will play a critical role in infrastructure modernization initiatives.
- Only 28 percent of respondents report that their agencies are currently compliant with MLS requirements to share classified information with organizations outside of their departmental boundaries.

...An IBM Solutions Impact Analysis

In response to these trends, IBM has integrated multi-level security support into its z/OS offering – a highly secure, scalable, high-performance enterprise operating system on which to build and deploy Internet and Java-enabled applications, providing a comprehensive and diverse application execution environment. Designed together with DB2 Version 8, IBM provides federal agencies with a high assurance solution for multi-level security on the zSeries mainframe. This support provides row-level security labeling in DB2, and protection in z/OS, designed to meet the stringent security requirements of cross-domain access to data. This solution leverages zSeries leadership in scale, high availability, and self-managing capabilities.

IBM's z/OS has been designed to comply with the Common Criteria Controlled Access Protection Profile (CAPP) at EAL3 and Labeled Security Protection Profile (LSPP) at EAL3+.

IBM's current MLS offerings take into account the need for a sustainable business case. The IBM business case is based on the current concerns of federal agencies and the desires for higher degrees of organizational integration. IBM is making the investments and partnering with government agencies as well as federal systems integrators to make these capabilities a reality.

Part 2: Market Impact Analysis National Security Requirements in the Post-9/11 Era

Today, the federal government must respond to new threats and undertake new missions in Internet time. The demand for concerted, coordinated action among military, intelligence and law enforcement agencies has never been greater, placing new and unprecedented stresses on the critical infrastructure of the national security community.

It has also placed new requirements for sharing sensitive information over a new more open architecture. For instance, new Department of Homeland Security (DHS) initiatives have significantly broadened the base of agencies and non-classified personnel that require access to sensitive data. Classified information must be broadly exchanged and jointly evaluated, leading to an explosion in the quantity of restricted files that must be shared.

Under these conditions, ensuring the integrity of that information and limiting its access to authorized personnel has become a significant challenge. Traditional boundaries between agencies are being taken down, and established efforts to compartmentalize data by agency and security level are proving inadequate for new mission imperatives. Thus, two trends are driving the development of more effective ways to secure the integrity of data, sources and methods based on the principles of multi-level security (MLS):

- New more flexible n-tier enterprise infrastructures that support Web Services are replacing legacy systems that kept automation initiatives “stove-piped” in their respective departments; and
- The new mission of the national security community calls for more effective sharing of real-time data in a secure manner.

...New Mission, New Requirements

As the complexities of ensuring data security have grown, the old approach of relying on fixed formats, rigorously controlled guards and stove-piped systems is no longer up to the task. The underlying technology has become too cumbersome to manage effectively; a new way of appropriately sharing data among larger groups of people at various levels of clearance is needed.

The traditional approach to enforcing Multiple Security Levels (MSL) is for each federal agency to operate a separate computing infrastructure for each level of security authorization in force at that agency. A discrete network with one set of servers and storage devices is deployed for top secret data; another is maintained for secret data and yet another for unclassified data (in some cases, all classifications of data are replicated on the servers with the highest security ratings). The total number of networks that must be maintained is a function of the number of security levels times the number of agencies with access to classified data. This makes for a very large number of networks and a very unwieldy infrastructure.

Multi-Level Security Strategies

Although costly and complicated, the MSL framework has provided a high degree of security assurance for intra-agency operations. But as the number and variety of *inter-agency* operations grows, the amount of data that must be exchanged among multiple networks with different levels of authorization increases geometrically, creating an untenable management burden. To ensure that the appropriate information reaches the appropriate people with a high level of assurance requires a more streamlined approach.

..Multi-Level Security

A better architecture for inter-agency data sharing is multi-level security or MLS. This approach dates back to the 1980s, when the Department of Defense (DoD) established guidelines and requirements for maintaining data processing security at its computing installations. These were published in the *Department of Defense Trusted Computer System Evaluation Criteria*, DoD 5200.28-STD, known more widely as TCSEC or the Orange Book, and they were applied to private companies working under government contract as well as to a broad spectrum of federal, state and local agencies.

Under these guidelines, computer systems were evaluated by the National Security Agency (NSA), and they received a designation ranging from D (least secure) to A1 (most secure), depending on the degree to which they adhered to the DoD criteria. These define a security policy that classifies data and users based on a system of hierarchical security levels. To this end, MLS has two primary goals.

- First, establish controls that prevent users from accessing information at a higher classification than their authorization permits; and
- Second, ensure that the controls prevent unauthorized users from declassifying information.

From an operational standpoint MLS offers tremendous advantages over the multiple security level strategy, because it does not require separate networks with separate servers in order to enforce different levels of security clearance. **Effectively implemented, MLS systems ensure that data can be consolidated onto a single infrastructure, while maintaining the highest levels of assurance that it can only be accessed by authorized users.**

Therefore, in this distributed computing and communications context an MLS-compliant system must have the following characteristics:

- The system must control access to resources.
- The system cannot allow a stored "shared resource" to be reused until it is purged of residual data.
- The system must enforce accountability by requiring each user to be identified and by creating audit records that associate security-related events with the users that initiate them.

Multi-Level Security Strategies

- The system must label all hardcopy and electronic data with relevant security information.
- The system must be able to hide the names of data sets, files and directories from users who do not have the “need-to-know” to access them.
- The system cannot allow an unauthorized user to declassify data by “writing down” to a lower classification than the classification at which the data was originally created.

...Barriers to MLS Implementation

Despite the promise of this approach, MLS has been slow to penetrate the intelligence and defense communities and has not spread beyond them to other federal agencies. There have been two major reasons for this.

- The types of security functions defined by MLS have not—in the main—applied to the private sector; and
- The Orange Book criteria only applied to U.S. agencies. While the governments of other nations had similar security requirements, they established their own separate security criteria.

These two factors have had the effect of significantly limiting the size of the MLS market for U.S. technology vendors. With only a few large government agency customers, the vendor community treated MLS as a niche or custom opportunity that was expensive to build and maintain over time.

...What's Changed?

A few developments over the past few years have significantly expanded the market opportunity for the vendor community, inducing leading companies like IBM and Oracle to expend more R&D dollars on MLS and to integrate the technology with their core product line.

- Many of the DoD Orange Book specifications have been internationally recognized and adopted – along with other standards – as a set of Common Criteria for multi-level security. This means that a system component that has been vetted by the National Information Assurance Partnership (NIAP) and assigned a security designation does not necessarily have to be resubmitted for compliance testing in each country (or agency) where it is sold under that same designation. This has greatly expanded the potential market for MLS and introduced economies of scale -- rapidly reducing the cost of fielding systems that comply with the security standards.
- The development of Web Services and the widespread adoption of the XML programming language have provided a new technical foundation for providing collaborative services in a heterogeneous technical environment. It is also

Multi-Level Security Strategies

creating significant opportunities to share data across organizational boundaries, which is creating demand for MLS services.

- The President's Management Agenda (PMA), which among other things calls for improved integration of activities across organizational boundaries, along with the adoption of industry-best-practices to streamline operations, is being applied to all agencies – including those tasked with national security-related missions.
- The nature of the war on terror has underscored the importance of real-time collaboration in response to threat developments, new intelligence information, and the dissemination of new analysis to all relevant response agencies.

The impact of these trends is documented by a joint **Larstan Business Report/Government Security News** survey of 214 security professionals working at federal agencies with a national security mandate. Respondents to the survey, which was conducted in late January, 2004, overwhelmingly agreed that the war on terror has increased the importance of information security (see Figure 1).

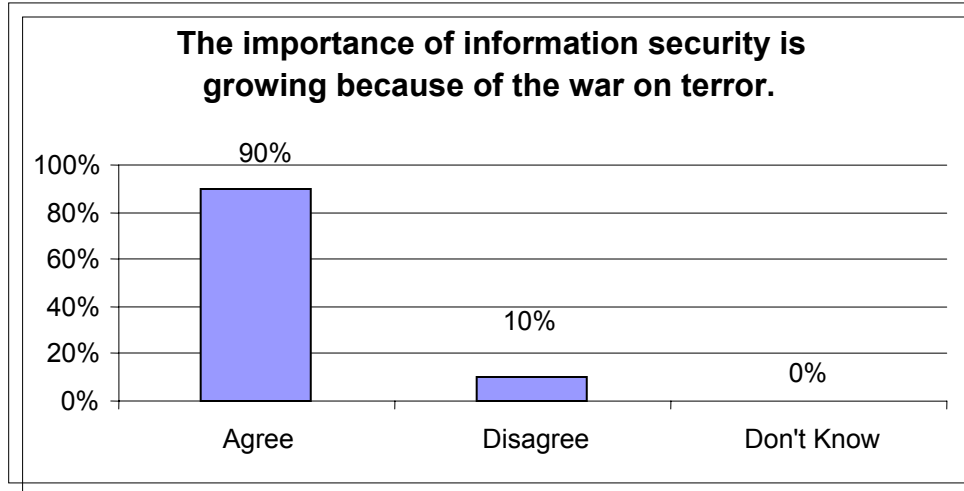


Figure 1 – Source: Larstan Business Reports/Government Security News

Closely related to this, the nation's new security posture is spawning an array of new eGovernment initiatives, which are also driving new information security requirements (see Figure 2).

Multi-Level Security Strategies

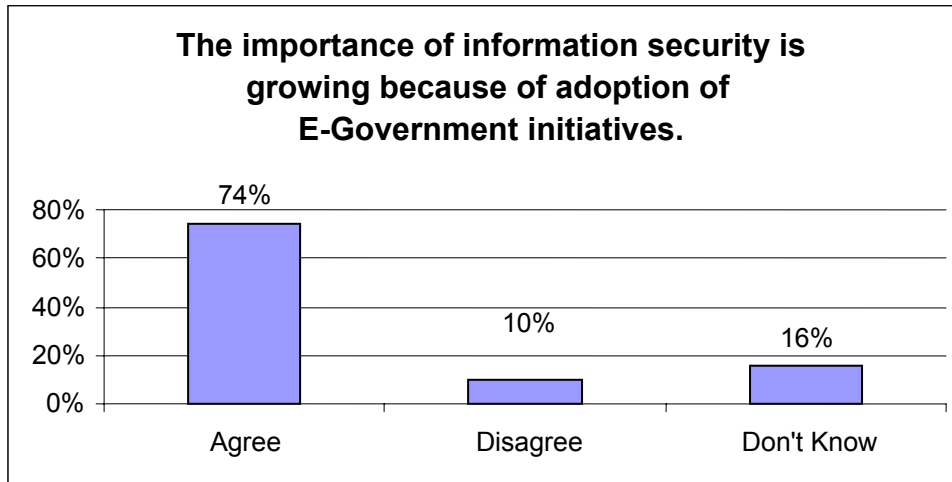


Figure 2 – Source: Larstan Business Reports/Government Security News

New security mandates and increased agency collaboration are reawakening interest in MLS. Just under two-thirds of the survey respondents indicated that their agency or department will implement MLS in order to securely share classified information with other agencies (see Figure 3).

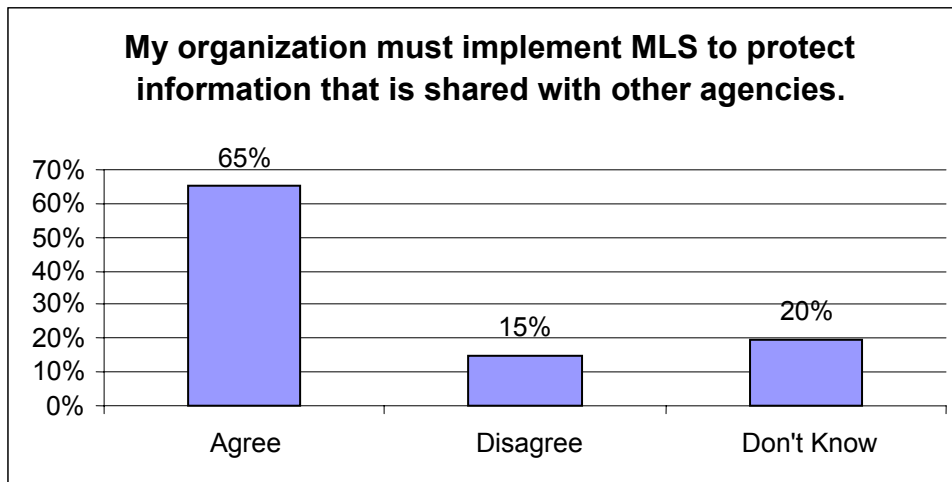


Figure 3 – Source: Larstan Business Reports/Government Security News

“MLS has been regarded as the Holy Grail for people operating in a high-assurance security environment . . . it was something that you deeply desired but could never really reach. Vendors treated it as a kind of one-off solution that you built once but never really continued with after that. That’s been a problem for government agencies that are wedded to an MLS capability that they bought a long time ago, but were never able to upgrade. IBM’s approach is different today. Our strategy now is to include and maintain it as part of our commercial-based systems, and to keep it current as we march forward in the future.” – Chris Daly, Practice Lead Federal Markets, IBM

Multi-Level Security Strategies

Part 3: Operational Impact Analysis Creating a Security Utility

If it were possible to profile the internal workings of a U.S. intelligence agency, as it struggles to meet new mission requirements, they might look something like this:

Intelligence agency X is a small agency whose primary objective was to gather and analyze very specific data associated with a very narrow portfolio. Traditionally it shared information cleared by its own gatekeepers with sister agencies in the intelligence and military communities and, on a very selective basis, with the State Department.

As the mandate of the intelligence community has shifted, agency X is now tasked with sharing information on a more dynamic and real time basis with key intelligence partners. But it is still critical to ensure that only authorized personnel can access the information.

The agency maintains top secret, secret, unclassified and a variety of other data classifications, which it enforces by maintaining discrete systems dedicated to different classifications and applying stringent controls to data replication. From an operational standpoint, this has necessitated a significant degree of content management, the extent of which is mounting rapidly, given the agency's new mission requirements. Agency heads recognize this and fear a security-compromising breakdown.

To alleviate its content management burden, agency X has concluded that it must migrate from its highly-stratified, stove-piped environment to a multi-level security architecture that supports a greater measure of data dissemination along with a high level of assurance. This will permit the agency to consolidate many of its servers onto a single platform, which enforces different security classifications using logical partitions and mandatory access control. Other security-related functions will include record auditing, user identification and name hiding.

The agency decided that the ideal platform is a mainframe that functions as an application database server. It will be complemented by a second server that uses Web Services to provide security for the applications and database, the operating system and portions of the network in a utility-like fashion. This will allow the agency to simplify and streamline its technology environment, and reduce its costs, while sharing information with other agencies in a secure and appropriate manner.

...Web Services and XML

The scenario described above depends on shifting the infrastructure's security functions onto a single dedicated server. This is accomplished through the marriage of MLS and Web Services.

MLS inserts security tags into the data stream to control access and audit usage. XML tags data in a universally recognized format, allowing the tags to be read and interpreted

Multi-Level Security Strategies

by otherwise incompatible systems. Using XML to create MLS security tags simplifies application development and expedites data exchange among disparate systems by applying the security function using industry standard technology. And by using digital signatures, agencies can ensure that the tag and the object being labeled are tightly bound – further ensuring the integrity and security of the data.

“To better access and integrate data, we’re talking about Web-based systems and XML-based interactions among systems. This is very much driven by the commercial market, but there is a strong desire now to employ these technologies with respect to the sharing and exchange of data among various security levels. So, one thing that’s quite obvious is that the old way of doing things, with fixed formats and very rigorously controlled guards and stovepiped systems, is unsatisfactory. The desire across the board within government, including state and local government, is to make sure that any new system does the sharing with these contemporary technologies.” – Eric Beyer, Lockheed Martin

From an operational standpoint, the implications of integrating MLS with Web Services are as follows:

- The MLS architecture provides the foundation for adopting Web Services through the use of XML security tags, which greatly simplify MLS implementation. Other XML tags can be used for a variety of secured Web Services, enabling federal agencies to share resources and exchange data more easily. Implementing Web Services is also an essential step for any agency looking to deploy the latest generation of commercially available technology.
- MLS-based Web Services pave the way for platform consolidation by allowing agencies to treat security in a utility-like fashion. Security functions once inserted in a system’s application code are now ‘stripped out’ and replaced by security services (in the form of XML tags), which are served up by a specialized Web server.
- Extracting the ‘security predicate’ from the core application code streamlines the application programming process, freeing agency IT staff to respond more quickly to new mandates and mission imperatives. It also eliminates the need for a separate security review for each new piece of application code, since the security functions are now performed by a single, isolated system.
- By imbedding the security functions in the system logic and architecture there is no longer any need to maintain separate physical systems to support different levels of security classification. Instead, these can be maintained through logical partitions and mandatory access controls, permitting agencies to consolidate most of their systems onto a single platform. This can dramatically reduce costs and data management overhead, while raising assurance levels and improving data access in a highly controlled manner.
- For larger agencies, the best platform for system consolidation is a robust, MLS-compliant mainframe. The mainframe is the most mature platform in the MLS-

Multi-Level Security Strategies

capable world and the most stable platform in the computing pantheon. It also offers the richest array of management features and the greatest economies of scale.

- With the right resources in place, larger agencies can adapt the commercial outsourcing paradigm to an eGovernment model and host systems for smaller agencies. Once again, MLS is the key enabler, since it provides a framework for walling off one agency's data from another's. Commercial outsourcers are likely to adopt MLS for the same reason—it will allow them to reduce their costs by hosting multiple accounts on a single platform and still guarantee high levels of privacy.

...A National Security Infrastructure in Perpetual Transition

It would be fair to characterize the national security community of agencies in the federal government to be early adopters of IT and communications technology in general, and security advances in particular. In fact, this segment of the government has tackled problems and created solutions that have been effectively transferred to the private sector. It would also be fair to say that this community of agencies is constantly monitoring and improving its infrastructure to accommodate the latest proven technologies

This fact is borne out in our survey. Sixty-five percent of the respondents indicated that their agency is currently engaged in modernizing its infrastructure. Only a small minority of respondents reported that their agency was not undertaking a modernization initiative (see Figure 4).

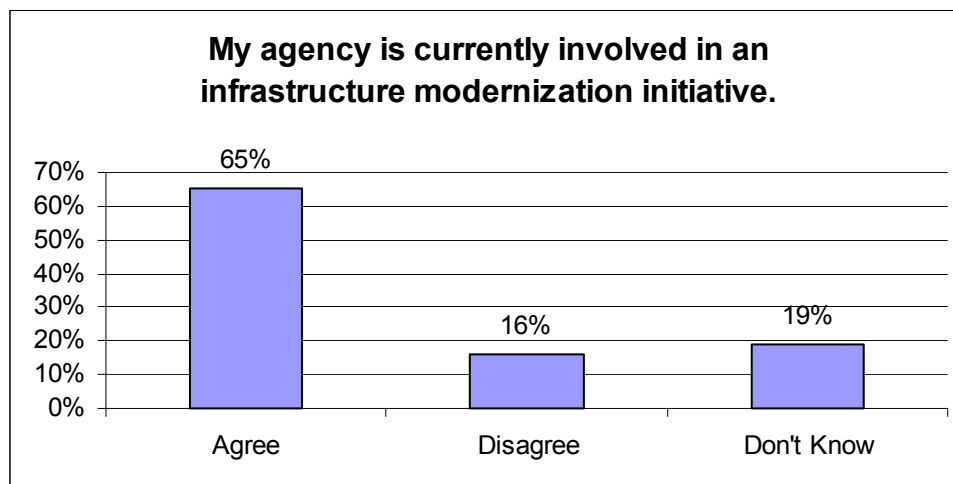


Figure 4 – Source: Larstan Business Reports/Government Security News

MLS implementation, according to a plurality of the survey respondents, is the driving force behind their agencies' modernization initiatives (see Figure 5).

Multi-Level Security Strategies

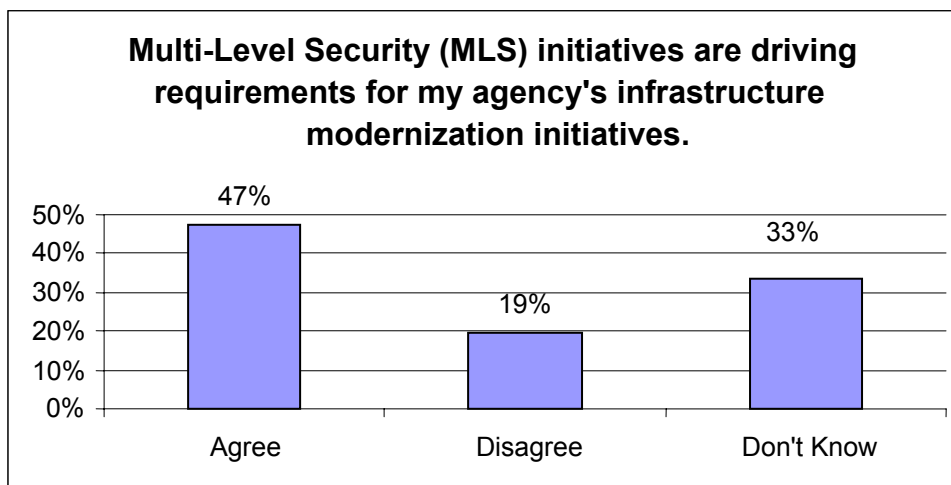


Figure 5 – Source: Larstan Business Reports/Government Security News

There is also recognition by larger agencies that the mainframe provides an optimal platform for large-scale systems consolidation. This is less applicable to smaller agencies and is reflected in the responses fielded by the survey (see Figure 6).

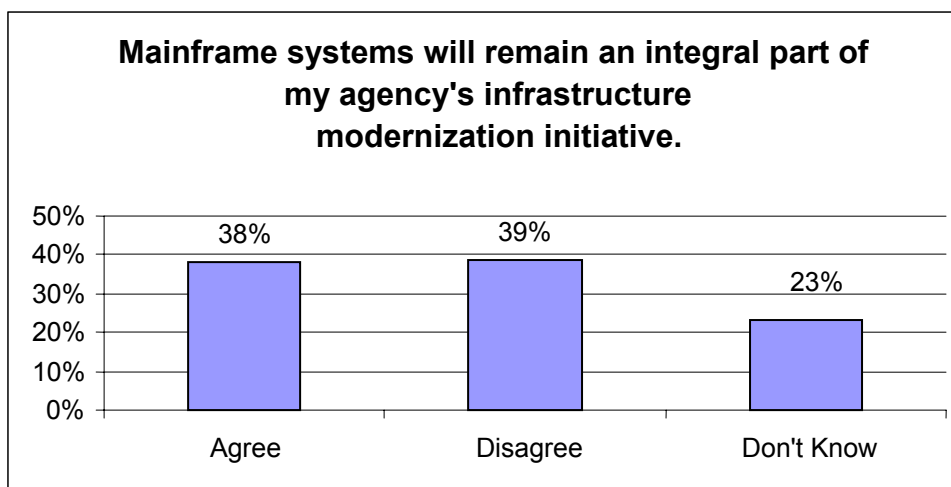


Figure 6 – Source: Larstan Business Reports/Government Security News

*“There are E-Government initiatives; there’s DHS, which needs to consolidate systems; there are several agencies that were lumped together and need to pull costs out of their equation, and there are various agencies that are interested in providing E-Services for other agencies. They are all starting to understand that in order to integrate their systems and reduce costs, but still meet the security and privacy that their missions require, they need an MLS infrastructure. It provides the underlying engine for e-business on demand for federal agencies.” – **Chris Daly, Practice Lead Federal Markets, IBM***

Multi-Level Security Strategies

Part 4: Security Impact Analysis MLS Characteristics and Compliance

“The government has raised the bar, and we are answering the challenge to develop effective technology that is needed to address the information sharing problem. The biggest nut to crack revolves around the level of assurance needed to guarantee that an individual’s access to the system from a lower level is consistent with a mandatory access control (MAC) policy. We want to be assured they will see only what they are supposed to. For this we need policy-based, rule-based access and rock-solid data management which guarantees that when I connect into that database server, I can only see what I’m supposed to see.” – Eric Beyer, Lockheed Martin

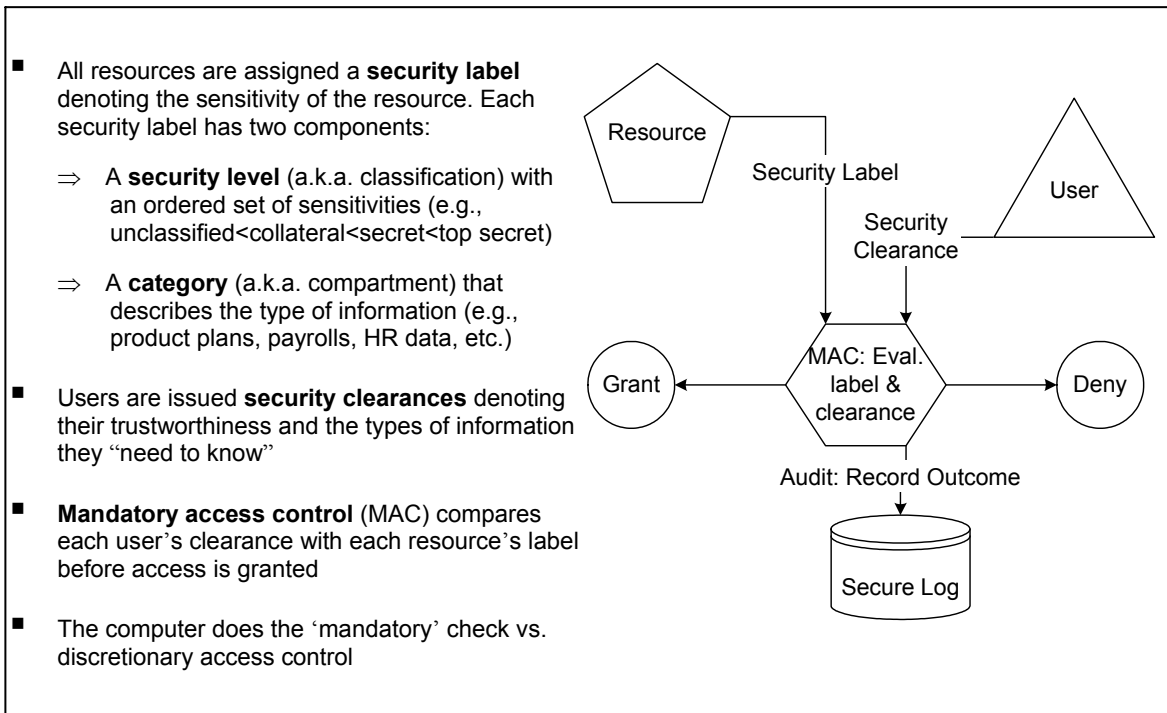
An MLS environment operates according to a set of rules and assurances that limit data access to authorized users and create an audit trail to maintain accountability. The chief control functions are as follows:

- **Mandatory access control (MAC)** – With mandatory access control, access is restricted based on the sensitivity of the information and the authorization of the user. These controls cannot be bypassed or altered by anyone other than an authorized security administrator. Security labels (tags) are used to define the sensitivity of each file or data object. The label denotes the level or classification of the information (such as top secret, secret, sensitive, etc.), and indicates to which category within that level (such as Project A or Project B) the information belongs. Security administrators also assign security labels to users, who can only access or enter data that is labeled at the same or at a lower level.
- **Discretionary access control (DAC)** – In addition to mandatory controls, MLS systems allow for some degree of discretionary access control. This is accomplished through the use of access control lists that identify the users that can access a given resource and their level of authority (e.g. read, update, delete) with regard to that resource. Both the resource owner and the security administrator can determine who can access the resource and with what authority.
- **Auditing** – Audit records associate security-related events (such as file access) with the user that caused the event. The audit record uses the security label to show when the data was accessed, the level of authority that was required and the actions that were taken.
- **Identification and authentication** – Each MLS system user is assigned an identity that corresponds to that user’s security label. Typically, user identities are verified through the Logon and Logoff commands and are used to maintain the audit trail.
- **Hardcopy labeling** – In an MLS environment, the system prints a security notation indicating the security level on each page of hardcopy output. It also creates corresponding electronic labels for the data file.

Multi-Level Security Strategies

- **Name-hiding** – The names of files, data sets and directories are only displayed to users with access authority. Users without a “need-to-know” will not see the file or object listed or displayed.
- **Write-down prevention** – To prevent users from declassifying data, an MLS system prohibits users from writing new data at a lower level of classification than their own label designation. In other words, a user with a top-secret classification can only create new data with a top-secret label. The user cannot ‘write down’ the data by labeling it secret or sensitive, in order to grant access to users with less than a top-secret designation.

MLS at a Glance



- **Row-level security** – Relational database users can be restricted to a specific set of rows by assigning each row a security label. Users with lower designations can still perform queries against the database, but the query results will not include any data from rows classified above that users’ security designation. This permits databases to be shared by users with various levels of security clearance without limiting the database to less sensitive data or compromising any highly sensitive data that it may contain.
- **Federated queries** – Users can issue queries across multiple databases and then store the combined results in an MLS database, which assigns them the appropriate security designation. Other users with varying levels of security classifications can query the MLS database and access data cleared for their level of clearance.

Multi-Level Security Strategies

- **Bit-map checks** – All resources and devices within an MLS environment receive a security label. Bit-map checks are performed against requests to use the device. For example, if a print request by an authorized user is made to print a top secret document on a particular printer, a bit map check will compare the device's clearance level with the document's. If they match, permission will be granted; if not, it will be denied.

...Confusion about MLS Reigns

Despite the considerable efforts that have gone into creating an MLS standard and deploying its functional capabilities to support today's distributed/collaborative infrastructures, a tremendous amount of confusion still exists about its impact on current organizations.

Our survey indicates that many federal security administrators are still unfamiliar with MLS. Less than a third of federal agencies report that their current security initiatives are MLS compliant (see Figure 7).

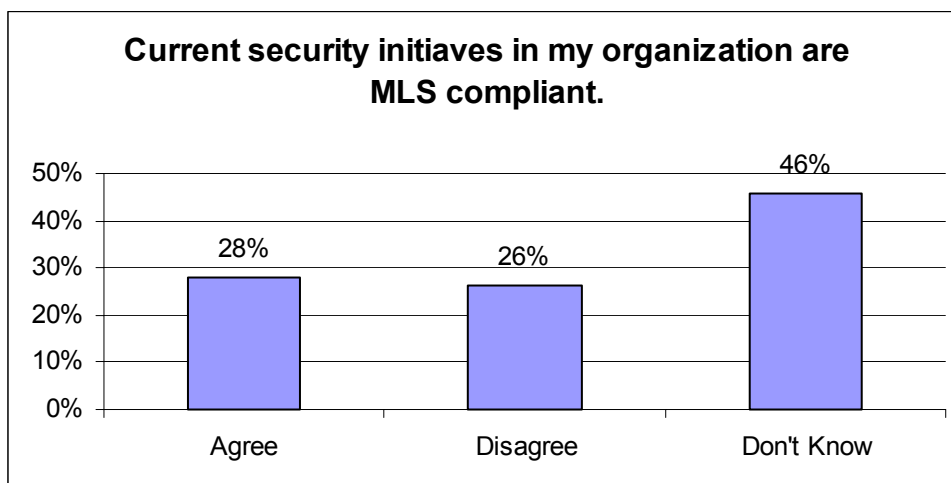


Figure 7 – Source: Larstan Business Reports/Government Security News

However, the survey results also show that MLS compliance will grow rapidly over the next eighteen months. As this happens, security administrators throughout the federal government are likely to become more familiar with the issues surrounding agency collaboration and multi-level security (see Figure 8).

Multi-Level Security Strategies

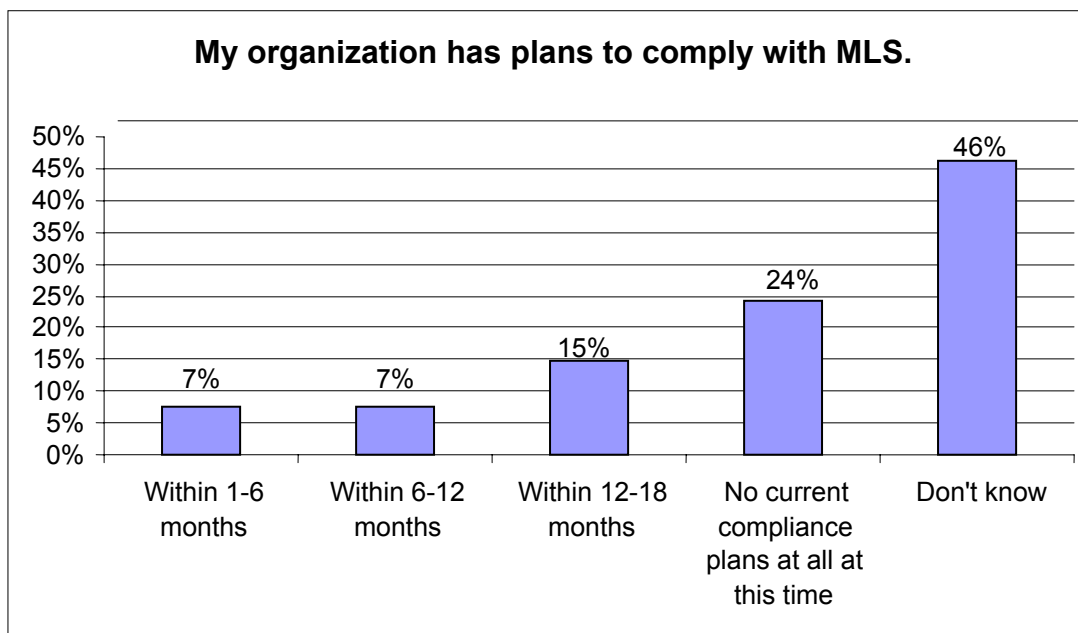


Figure 8 – Source: Larstan Business Reports/Government Security News

Already, among those respondents whose agencies are currently engaged in infrastructure upgrades, fifty percent of the respondents report that MLS is an integral aspect of their modernization efforts (see Figure 9)

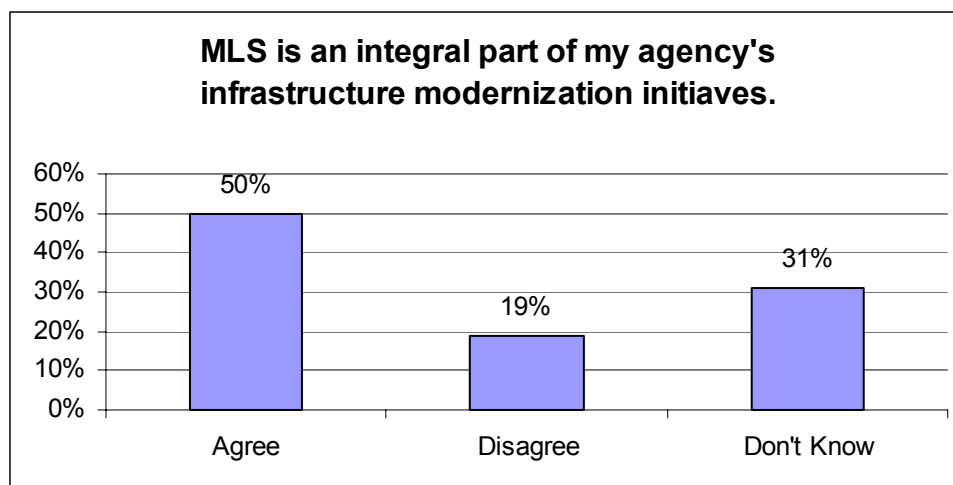


Figure 9 – Source: Larstan Business Reports/Government Security News

...Conclusion

Despite the 20 year history of MLS, both the empirical and anecdotal evidence suggest that pace of MLS-compliant systems deployment will pick up speed. It is fair to predict that a faster rate of MLS adoption will begin in 2004, and that the deployment of MLS will not only coincide with, but enable, the implementation of collaborative infrastructures that require the secure exchange of the most sensitive information in the nation in a distributed computing environment.

Multi-Level Security Strategies

As agencies modernize their systems, re-engineer their business processes, and consolidate their technology assets, it will be important to select infrastructure platforms that can support MLS requirements, as well as provide a unified foundation from which classified information can be disseminated and stored.

The mainframe platform promises to play an increasingly important role in supporting the migration to an MLS-compliant infrastructure, as agencies look for cost-effective and secure ways to integrate systems appropriately across organizational boundaries while managing the complexity of their enterprise systems.

However, it is also clear that much needs to be done to take the mystery out of MLS. The fact that a full 46% of respondents in the national security community are unsure of what their MLS plans are indicates a gap between a high level awareness of what MLS is, and the specific knowledge required to rapidly and effectively deploy this security standard in their organizations.

Because MLS plays an integral role in how the national security community shares classified information securely across organizational boundaries, establishing a clear strategic, operational and technical road map to MLS compliance will be a high priority for IT and security professionals in these agencies.

Multi-Level Security Strategies

Part 5: Solutions Impact Analysis IBM Delivers MLS with Mainframe Qualities of Service; z/OS and DB2 MLS Designed to Meet Common Criteria Standards

The need to share information among different governmental agencies has risen dramatically due to the war to combat terrorism. This increased emphasis on information-sharing has placed greater responsibilities for handling national security information on local and federal agencies that, in the past, have been outside the normal channels of classified information processing. This has prompted urgent interest in the capabilities offered by multi-level security (MLS) standards since it supports collaborative operations among multiple agencies.

There has been a simultaneous trend in the federal government to consolidate and simplify the extremely complicated and splintered enterprise infrastructures of most agencies tasked with national security responsibilities. As agencies move to consolidate enterprise resources and improve performance to support the collaborative imperatives associated with today's national security missions, mainframe computing platforms are shaping up to play an increasingly important role.

The ability to coalesce classified information sharing onto consolidated infrastructures provides significant cost savings for these agencies, while also helping to streamline DoD and intelligence community infrastructures that must connect to many more locations and agencies. IBM's approach to supporting MLS is designed to address these challenges.

...IBM's Approach to MLS

IBM has integrated multi-level security support into its mainframe operating system, z/OS Version 1 Release 5. Designed together with DB2 UDB for z/OS Version 8, z/OS provides federal agencies with a high assurance solution for MLS on the zSeries mainframe. This support provides row-level security labeling in DB2, and protection in z/OS, designed to meet the stringent security requirements of cross-domain access to data. This solution leverages zSeries leadership in scalability, high availability, and self-managing capabilities.

IBM's z/OS has been designed to comply with the Common Criteria Controlled Access Protection Profile (CAPP) at EAL3 and Labeled Security Protection Profile (LSPP) at EAL3+. Presently, z/OS is under evaluation to meet this specification.

Consequently, the zSeries mainframe solution from IBM can address government requirements for highly secure data exchange. New security features in DB2 V8 and z/OS 1.5 enable agencies to have a single highly secure repository of data that has different sensitivity attributes and which can be accessed by different agencies and by people with different clearance levels. This secure access is managed at the row level in DB2 to provide the granularity that is required.

“Our competitive advantage with MLS—and I'm really talking about generic MLS—is that we use the same security server for the database as we do for the operating system and some of the network communications. Therefore change management on any one of those parts is simplified because you are still

Multi-Level Security Strategies

preserving that centralized security manager.” – Jim Porell, Chief Strategist zSeries software design, IBM

Consequently, agencies will be able to:

- Have faster access to merged inter-agency data
- Manage multiple security classifications
- Help eliminate the need for multiple infrastructures for managing cross-domain access of data

The zSeries platform can provide this MLS security for applications using the latest open industry standard technologies. The z/OS environment supports technologies such as Enterprise JavaBeans, XML, HTML, Unicode, distributed IP networking, and Public Key Infrastructure services (PKI). The z/OS UNIX System Services allows agencies to develop and run UNIX programs on z/OS and exploit the reliability and scalability of the IBM eServer zSeries servers. It also supports distributed print services, storage management, and advanced workload management capabilities.

Since zSeries customers are some of the largest and most security-sensitive organizations in the world, security has always been an important component of the zSeries strategy. Security is a key design point for zSeries servers, operating systems, middleware and applications.

The zSeries servers have implemented leading-edge technologies such as high-performance cryptography, large-scale digital certificate support, continued excellence in Secure Sockets Layer (SSL) performance and advanced resource access control function. With Intrusion Detection Services, zSeries has enhanced its ability to help resist network-based attacks while embodying industry and international standards.

- Also the Logical Partitions on zSeries z800 and z900 servers are certified to Common Criteria at EAL5. These servers are currently the only servers to have obtained this level of certification.
- Leverage zSeries Cryptography for Clear Key and Secure Key
- Deploy z/OS Security Server, including RACF

IBM's current MLS offerings take into account the need for a sustainable business case. The IBM business case is based on the current concerns of federal agencies and the desires for higher degrees of inter-organizational integration. IBM is making the investments and is establishing partnerships with government agencies and major contractors to make these capabilities a reality.

“MLS on z/OS can help an agency or multiple agencies simplify their computing infrastructure. Compartmentalizing their data, while also consolidating the data in a large database, like DB2 UDB for z/OS, should reduce much of their management complexity. Hosting this database on z/OS will provide scalability,, availability and efficient utilization levels that should meet and exceed the service level needs of most agencies.” – Jim Porell, IBM