New Email Security Infrastructure

Martin Ferris

U.S. Treasury

Abstract

Given the need for interorganizational electronic mail systems, a security infrastructure will be needed to administrate such systems. Using the U.S. government as a model, this paper examines policies that establish the status quo infrastructure for security and advocates policy for a new infrastructure.

Introduction

What national policy for the purpose of securing Electronic mail (Email) systems processing National Security information best satisfies the objectives of the National Information Infrastructure (NII)?

Although security policy implementation across the government unfolds through a slower, incremental process, the national policy for securing Executive Branch information systems comes from the White House (e.g. Executive Orders, National Security Decisions, Office of Management and Budget Circulars). The policy development mechanism for systems that process national security information is the political by-product of the National Security Telecommunication and Information Systems Security Committee (NSTISSC) which in NSD 42 is chartered by the National Security Council to develop, coordinate and promulgate such policy. The NSTISSC is supported by subcommittees and working groups consisting of Executive Branch departments. The Office of Management and Budget (OMB) promulgates general systems security policy for the non-National security Executive Branch departments. In both cases, policy is ultimately implemented on an agency-by-agency basis.

This analysis advocates a policy that creates a new infrastructure for processing interagency Email systems while using non-National Security standards to protect privacy within national security environments. The analysis also identifies differences between the security perspective and the cost and operations perspectives. Next steps are suggested to improve the successful acceptance and implementation of the policy.

Background

The White House has created an Information Infrastructure Task Force (IITF) to help formulate policies needed to accelerate the federal government's implementation of the NII. The IITF has agreed on the need for federal employees to access a government wide Email system and has commissioned an Email Task Force to recommend government-wide Email policy direction.

Electronic mail is one of the critical technologies in the realization of the NII. Government-wide Email is an underlying element of the Administration's vision for the NII and is an enabling technology to achieve many goals expressed in the administration's National Performance Review (NPR) initiatives. The NPR views government-wide Email as essential to implement President Clinton's commitment to " fundamentally altering and improving the way the Federal government buys good and services, and thus ensuring that electronic commerce is implemented for appropriate Federal purchases as quickly as possible."

There is a concern that the IITF Email Task Force's security policy recommendations will be weak; serving only as the lower boundary for acceptable security. While a weak security policy recommendation would offer a quicker implementation of electronic commerce with less technical and administrative obstacles while, from the perspective of others, it will place at risk privacy and other security-related concerns that could later require expensive security corrections.

Status quo infrastructure

An infrastructure currently exists for Federal Agencies to secure their sensitive information (National Security or non National Security) commensurate with risks to the information. The infrastructure consists of both administrative and technical parts. Administratively, it is left to a federal agency's discretion as to the level of security that they deem appropriate. Each agency will comply with national policies for managing risks (i.e. OMB Circular A-130, privacy laws, federal records management laws and policies and NSTISSC issuances) through the issuance of internal policy directives and standard operating procedures. As each agency assesses the risks to its own operations (e.g. compromise of classified information, financial fraud, unauthorized access to privacy information), the agencies decide whether security is necessary and, if so, how much is appropriate for each situation.

The technical portion of the infrastructure is realized through the availability and implementation of the technical standards (i.e. Federal Information Processing Standards, NSTISSC standards) for the protection of the sensitive information. Systems security standards can be applied to achieve varying levels of assurance in the management of risks. High levels of assurance would include the application of encryption for strong confidentiality or authenticity (i.e. digital signatures) protection of sensitive information. High levels of assurance typically require more special technology that results in higher costs (i.e. technology costs and administrative costs). Both high and low assurances are required by the government as various agencies decide their risks and make security decisions.

Analysis

The technical and administrative infrastructure previously stated is the Status Quo for the US government. As long as information security issues are considered internal agency issues, the status quo infrastructure is adequate. However, the NII will challenge the government's Status Quo infrastructure for effectively managing risks to data privacy and integrity because the Status Quo does not address interagency information systems and services (e.g. interagency Email systems). Within a government-wide Email environment, the decision whether security services are necessary and, if so, how much and what kind is required, will not always be at the discretion of an individual agency.

Who will choose which security standards to use? Who will assure that the technology will be interoperable? Who will decide which records are official government records? Who will decide what level of security assurance is adequate for the privacy protection requirements of different agencies? Who will receive the interagency funding for implementation?

Government-wide Email demands that the government, including the national security community, ask whether the existing infrastructure satisfactorily accommodates interagency systems or whether policy action is required to either assist the existing infrastructure to change or require a new infrastructure? If a new infrastructure is decided as necessary, which US government agency should be assigned responsibilities to create and manage the new infrastructure?

Under the National Security Directive (NSD)42, the Director National Security Agency (NSA) serves as the National Manager for community information systems security issues. The Secretary of Defense is the Executive Agent for implementing National Security Directive 42. Currently, NSA and the Department of Defense (DOD) have undertaken technology initiatives (i.e. Defense Message System) that could serve as the technical infrastructure for the National Security communities and a proactive model for securing government-wide Email.

Since the NSTISSC has a charter to establish security policy for National Security community and since National Security environments process non National Security information also, an NSTISSC direction would assist the IITF by more fully framing the broader security policy recommendations.

The NSTISSC could:

1. Issue Email security policy to resolve the infrastructure issue for those systems that process National Security information only; or

2. In addition to the above, acknowledge that some of the National Security community's security requirements such as privacy and electronic signature can be met by using non-National Security (i.e. FIPS) standards.

Analysis technique

The above provides a basis for choosing policy alternatives for consideration by the SISS's Secure Email Working Group. The alternatives should satisfy the objective of an infrastructure that provides the National Security community with the necessary security services for the full range of security and privacy needs; while supporting the quickest realization of the NII at the lowest cost and with the least operational impact. The Criterion Analysis technique is chosen to identify the best security policy alternative while considering three often conflicting perspectives (i.e. operations, security and OMB). The three perspectives are intended to assist in obtaining a consensus in formulating a secure Email policy for the Secure Email Working Group.

Policy alternatives

The following are four alternative policy actions to be considered. Their descriptions and rationales, the criteria by which the policy alternatives are evaluated, and their assessment scores are included. The assessment results are included as appendices. The assessment results are the projection of this paper's author.

ALTERNATIVE 1 - Status Quo: The current infrastructure does not need to change.

Advantages:

The operations and OMB perspectives would value this alternative. The OMB and operations perspective may consider interagency problems as matters that agencies can handle internally without central government interference.

Disadvantages:

The security perspective would see this alternative as limiting the advancement of Email since it does not directly resolve interagency problems. From a security perspective, this is not proactive in assuring availability of widest range of security services.

ALTERNATIVE 2 - Status Quo plus Evaluations: The infrastructure should remain the same but improve the agency security decision process by requiring agencies to evaluate their application of security for performance and results overtime to determine intended results are achieved.

Advantages:

The OMB perspective would prefer this alternative since the it would facilitate a more careful determination of the need for additional security assurances. Also, since the Government Performance and Results Act applies to the National Security operations, this alternative gives OMB a pilot opportunity for National Security community implementation.

This alternative also would be favored by OMB and operations because security decisions would be more cautious about implementation of security and, consequently, budget expenditures for security would be more conservative.

Disadvantages:

Although the evaluations would be useful, the security perspective would be similar to Alternative 1 in that Alternative 2 is not proactive in assuring availability of the widest range of security services.

ALTERNATIVE 3 - Infrastructure with Classified Only Focus: The National Manager is assigned responsibility for establishing a security infrastructure by 1997. The infrastructure would apply to electronic message systems processing classified information only.

Advantages:

This alternative establishes a new infrastructure model for the government as far as classified information is processed across agencies. From an operations and security perspective, this would provide the most flexible and would be most responsive to the widest range of classified security requirements. The fear of excessive cost and loss of control by operations may result in the lack of full support for this alternative. Furthermore, this option will create faster implementation of electronic commerce for National Security environments (e.g. industrial security).

From an OMB and operations perspective, cost-savings should be attractive to OMB and operations if the National Security community can use DOD "sunk costs" in the Email infrastructure.

Disadvantages:

The time required for the classified versions of Email security technology is longer and the application of National Security standards to privacy and non-repudiation may be more complicated than using non-National Security standards.

The use of National Security standards would generate higher cost because of limited user population.

ALTERNATIVE 4 - Infrastructure For Classified and Inclusive of non-National Security standards: This option modifies Alternative 3 by requiring NSA to use non-National Security standards to achieve privacy objectives.

Advantages:

This option establishes a comprehensive new infrastructure model for the government to secure Email systems with the most flexibility and responsiveness to the widest range of classified and non-National Security requirements.

This option will facilitate the fastest implementation of electronic commerce, where high security assurances have been determined to be a requirement.

Assumptions

Agencies will continue to determine their own privacy and other application security requirements. All necessary security technology is either currently available or available within two years. Cryptographic service technology includes: all necessary cryptographic techniques for confidentiality, integrity and, when combined with administrative procedures, non-repudiation, and protocols for the negotiation of the minimum security services.

For Alternative 3,

It is assumed that the National Manager will accept assigned responsibilities to provide cryptographic service technology that can accommodate National Security standards only.

For Alternative 4,

It is assumed that the DOD will accept assigned responsibilities to provide interagency classified Email system and serve as Email provider of last resort for the National Security community.

Also, it is assumed that the National Manager could also be assigned responsibilities to provide cryptographic service technology that uses non-National Security standards for the protection of privacy information.

Criteria

The following is the criteria by which the Alternatives will be assessed along with weights and rationale for each criterion:

1. Implement Electronic commerce as quickly as possible - Electronic commerce is a major political priority of the Administration and is given weight of 10. OMB types will want electronic commerce implemented with less controls while security types will assume that a successful implementation of electronic commerce will be risk, without the full range of security assurances made easily available.

2. Minimize operational pain - Technology is supposed to make life easier. Security and evaluations are extra work and tremendous resources. This is important for policy acceptance and quick implementation. OMB wants electronic commerce to be implemented quickly. This is given a weight of 9.

3. Ease of implementation near term - Ease of implementation will be quickly perceived by operational implementors and is critical to acceptance of any policy alternative by operational types. A weight of 8 is given for security and operations perspectives while a weight of 9 is given for the OMB perspective.

4. Ease of implementation long term - Same as above but for the long term a greater opportunity to achieve acceptance of the policy is possible. A weight of 6 is given.

5. Flexibility for additional security - This is highly important from a security perspective. This is given a weight of 10. This is not as important to OMB or operations perspectives where a weight of 8 is given.

6. Responsive to widest privacy needs - This a major administration issue and is given a weight of 10.

7. Least costly - This is important to OMB but not as important to security or operations. It is given a weight of 7 from a security perspective while it is given a weight of 10 for operations and OMB perspectives.

8. Responsive to agency budget - This is very important from a OMB perspective but not as important to security. This is given a weight of 7 for security and operations perspectives but from an OMB perspective a weight of 9 is given.

9. Maximizes agency decisions - Since agency ownership of security issues is important to the success of security as well as agency acceptance of a policy, a weight of 7 is given. The OMB perspective would agree because this provides best risk management decisions and associated budget decisions. Operations would value agency decision ownership the most of the three perspectives, where a weight of 10 is given.

Conclusions

From a security perspective the analysis indicates that Alternative 4 would be the preferred policy direction. Also, the analysis indicates Alternative 4 would be expected to receive strong support from an operations perspective. Alternative 4 is not expected to receive strong support from the OMB perspective.
With this understanding, the next steps would be to present the analysis to the Chair of the SISS with the following recommendations;

o Validate reasonableness of Analysis (i.e. weights, alternatives) with the Secure Email Working Groups;

o Validate technical and political realities of all assumptions;

o Test the acceptability (e.g. SISS members, NSA, NIST, OMB) of having the National Security community accepting non-National Security standards for privacy matters;

o Create a draft policy based on Alternative 4 for the Secure Email Working Group's review and comment;

o Include the evaluation requirement/ of Alternative 2 in the draft policy since this has received strong support from OMB and Operational perspectives; and

o Share the analysis with the IITF Email Task Force for comment.

Finally, assuming that Alternative 4 is accepted as the policy for securing National Security Email systems, the National Manager needs to consider the prioritization of the security services that would be offered to best serve the users at the lowest cost.

OPERATIONS CRITERIA	WEIGHTS	STATUS QUO	STATUS QUO PLUS EVALUATE	INFRA-STRUCTURE	EXTRA INFRA-STRUCTURE
Electronic commerce as quickly as possible	10	5 / 50	6 / 60	10/ 100	7 / 70
Minimize operational pain	9	10 / 50	9/ 81	5 / 45	7 / 63
Ease of implementation near term	8	10 / 80	9 / 72	6 / 48	8 / 64
Ease of implementation long term	6	4 / 36	5 / 45	7 / 42	9 / 54
Flexibility for additional security	8	6 / 48	7 / 56	7 / 56	10 /80
Responsive to widest privacy needs	10	7 /70	10/100	6 / 60	9/ 90
Least costly	7	6 / 42	9 / 63	7 / 49	10 /70
Responsive to agency budget	7	6 / 42	9 / 63	7 / 49	10/ 70
Maximizes agency decisions	10	5 / 50	10/100	7 / 70	8 / 80
TOTAL		468	**640**	519	**641**

APPENDIX 1

SECURITY CRITERIA	WEIGHTS	STATUS QUO	STATUS QUO PLUS EVALUATE	INFRA-STRUCTURE	EXTRA INFRA-STRUCTURE
Electronic commerce as quickly as possible	10	4 / 40	5 / 50	7 / 70	10 / 100
Minimize operational pain	9	10 / 90	8 /72	7 / 63	7 / 63
Ease of implementation near term	8	10 / 80	9 / 72	8 / 64	8 / 64
Ease of implementation long term	6	4 / 36	5 / 45	9 / 54	10 / 60
Flexibility for additional security	10	4 / 40	6 / 60	7 / 70	10 /100
Responsive to widest privacy needs	10	5 / 50	8 / 80	9 / 90	10 / 100
Least costly	7	3 /21	6 /42	7 /49	10 / 70
Responsive to agency budget	7	4 /28	7 /49	5 / 35	10 /70
Maximizes agency decisions	7	2 / 14	4 / 28	9 / 63	10 / 70
TOTAL		399	498	558	**697**

APPENDIX 2

OMB CRITERIA	WEIGHTS	STATUS QUO	STATUS QUO PLUS EVALUATE	INFRA-STRUCTURE	EXTRA INFRA-STRUCTURE
Electronic commerce as quickly as possible	10	8 / 80	10/100	6 / 60	5 / 50
Minimize operational pain	9	8 / 72	10 /90	7 / 63	5 /45
Ease of implementation near term	9	10/ 90	9 / 81	6 / 48	5 / 45
Ease of implementation long term	6	9 / 54	10/ 60	6 / 36	5 / 30
Flexibility for additional security	8	9 / 72	10 /80	7 / 56	6 / 60
Responsive to widest privacy needs	10	9 / 90	10/100	5 / 50	6 / 60
Least costly	10	10/100	9 / 90	6 / 60	4 /40
Responsive to agency budget	9	9 / 81	10 /90	6 / 54	5 /45
Maximizes agency decisions	7	9 / 63	10/ 70	8 / 56	8 / 56
TOTAL		702	**761**	483	431

APPENDIX 3