Implementing a Trusted Information Sharing Environment

Using Immutable Audit Logs to Increase Security, Trust, and Accountability

A PAPER BY THE MARKLE TASK FORCE
ON NATIONAL SECURITY IN THE INFORMATION AGE

ZOË BAIRD, JAMES BARKSDALE
CHAIRMEN

MARKLE FOUNDATION

MARKLE FOUNDATION

TASK FORCE ON NATIONAL SECURITY IN THE INFORMATION AGE

MEMBERS AND ASSOCIATES, 2006

Chairmen

Zoë Baird
Markle Foundation

Jim Barksdale
Barksdale Management Corporation

Members

Robert D. Atkinson
Progressive Policy Institute

Eric Benhamou
3Com Corporation, Palm, Inc., Benhamou Global Ventures, LLC

Jerry Berman
Center for Democracy & Technology

Robert M. Bryant
National Insurance Crime Bureau

Ashton B. Carter
Kennedy School of Government, Harvard University

Wesley Clark
Wesley K. Clark & Associates

William P. Crowell
Security and Intelligence Consultant

Bryan Cunningham
Morgan & Cunningham LLC

Sidney D. Drell
Stanford Linear Accelerator Center, Stanford University

Esther Dyson
CNET Networks

Amitai Etzioni
The George Washington University

David J. Farber
Carnegie Mellon University

John Gage
Sun Microsystems, Inc.

John Gordon
United States Air Force, Retired

Slade Gorton
Preston Gates & Ellis LLP

Morton H. Halperin
Open Society Institute

Margaret A. Hamburg
Nuclear Threat Initiative

John J. Hamre
Center for Strategic and International Studies

Eric H. Holder, Jr.
Covington & Burling

Jeff Jonas
IBM

Arnold Kanter
The Scowcroft Group

Tara Lemmey
LENS Ventures

Gilman Louie
Alsop Louie Partners

John O. Marsh, Jr.
Marsh Institute for Government and Public Policy, Shenandoah University

Judith A. Miller
Bechtel Group, Inc.

James H. Morris
Carnegie Mellon University

Craig Mundie
Microsoft Corporation

Jeffrey H. Smith
Arnold & Porter LLP

Abraham D. Sofaer
Hoover Institution, Stanford University

James B. Steinberg
Lyndon Johnson School of Public Affairs, University of Texas at Austin

Paul Schott Stevens
Investment Company Institute

Rick White
former Member of Congress

Associates

Laura Bailyn
Skadden, Arps, Slate, Meagher & Flom LLP

Rand Beers
Coalition for American Leadership and Security

Bruce Berkowitz
Hoover Institution, Stanford University

Scott Charney
Microsoft Corporation

Bob Clerman
Mitretek Systems

Jim Dempsey
Center for Democracy & Technology

Mary DeRosa
Center for Strategic and International Studies

Richard Falkenrath
The Brookings Institution

David Gunter
Microsoft Corporation

Drew Ladner
JBoss, Inc.

Randolph D. Moss
Wilmer Cutler Pickering LLP

Bill Neugent
MITRE

Daniel Prieto
Kennedy School of Government, Harvard University

Clay Shirky
Writer and Consultant

Peter Swire
Moritz College of Law, The Ohio State University

Kim Taipale
Center for Advanced Studies in Science and Technology Policy

Mel Taub
Independent Consultant

Richard Wilhelm
Booz Allen Hamilton

Director , National Security Program

Linda Millis
Markle Foundation

Markle Foundation Staff

Karen Byers
Managing Director and Chief Financial Officer

Kim Hogg
Assistant to the President

Michelle Maran
Manager, Public Affairs

Danielle Petras
Project Assistant, Task Force on National Security in the Information Age

Stuart Schear
Director of Communications, Health and National Security Programs

Stefaan Verhulst
Chief of Research

Visualization Producer

Sean Dolan
LENS Ventures

Implementing a Trusted Information Sharing Environment

Using Immutable Audit Logs to Increase Security, Trust, and Accountability*

February 2006

A Project of

The Markle Foundation
New York City

* The Markle Foundation Task Force on National Security in the Information Age acknowledges and thanks Jeff Jonas and Peter Swire as lead authors of this monograph, as well as Daniel Prieto for initial editing.

Executive Summary

Widespread adoption of a trusted information sharing environment (ISE) requires that users have confidence in the security of the system. To promote confidence and trust in the ISE and to help govern information sharing, the ISE should incorporate robust security and audit features, including immutable audit logs (IALs). The ability to maintain tamper-resistant logs of user activity on the network can increase security, build trust among users, ensure compliance with relevant policies and guidelines, and improve transparency and the ability to perform oversight by appropriate stakeholders outside of the system.

Audit logs will record activity that takes place on the information sharing network, such as, for example, queries made by users, the information accessed, information flows between systems, and date- and time-markers for those activities. Making such logs immutable builds confidence that they accurately reflect actual activity and have not been altered. By providing thorough recordkeeping on the activities that occur within the ISE, officials can use IALs to demonstrate that sharing behavior complies with applicable laws and policies, and to detect violations. IALs will be a critical component for the ISE since improved and innovative sharing behavior will represent a marked departure from the current business and behavioral models typical within government.

ISE managers should ensure that IALs do not create their own security vulnerability by using encryption, ensuring that logs are never stored in a single location, strictly limiting access to logs, and subjecting everyone reviewing logs to audit.

Discussion and Analysis

It is essential to put in place effective safeguards and security measures to accompany greater sharing of sensitive information within the ISE. The Markle Foundation Task Force on National Security in the Information Age recommended a number of such measures in its 2003 report, *Creating a Trusted Information Network for Homeland Security* (available at www.markle.org). One powerful component of the ISE should be the ability to record system activity in IALs.

IALs are especially important for systems where there is limited transparency, such as the ISE, which contains classified government information. Without logging of user activity in such systems, there is no way to demonstrate clearly for oversight and accountability purposes that there is compliance with established policies and laws. The resulting lack of trust in institutional compliance can lead to a situation in which reasonable and desirable uses of information are blocked for fear that privacy and civil liberties protections may be violated, or that data could be misused. As such, IALs may represent an intermediate solution between public communication and total secrecy.

This paper seeks to provide insight into the use of IALs for the ISE by exploring the technical, policy, and security issues relating to IALs. The paper explores some of the technical issues relating to IALs, including what can be logged effectively, the differences between mutable and immutable logs, and institutional barriers to deployment of IALs. It analyzes some of the potential benefits to the ISE of deploying IALs. At the same time, the paper recognizes some drawbacks, including the possibility that IALs may introduce new vulnerabilities. Finally, the paper offers policy recommendations.

The paper intentionally does not examine or discuss other potential and beneficial functions of a comprehensive logging system, which might include: monitoring system and network functionality, or system self-awareness (for example, to discover common interests among users, inform resource decisions, or improve analysis and reporting by contributing to a planning process).

A. Benefits of using IALs

Any audit—whether based on mutable or immutable logs—provides benefits, including the ability to deter, detect, and prove policy violations. The ability to perform audits within a system serves as a deterrent because system users will know in advance that logging and auditing are being used to identify policy violations. The perception that a system is effectively logged and will be audited may thus reduce violations by users. Detection occurs when an actual policy violation is uncovered after the fact. Detection may occur as a result of sampling, when one of the transactions selected for random audit reveals a violation. Detection may also occur in the context of a specific investigation, when the actions of a suspect are examined carefully and a violation is detected. Finally, audits can be used to create evidence of a violation. If there is a credible recordkeeping system in place, then records from the system can be convincing to those investigating and judging a case.

Typically, audit logs are maintained in the custody of a highly privileged system user, for example, a system administrator with authorized access. Logs are typically

mutable—that is, the system administrator (or others with appropriate privileges) can add, change, and delete log entries. Traditional mutable logs are also vulnerable to unauthorized tampering by a malicious party other than the system administrator. Indeed, changing logs is a standard procedure for both inside and outside hackers in order to hide evidence that would reveal their unauthorized activity.

To address deficiencies of trust in mutable logs, immutable logs require either that log information cannot be altered by anyone regardless of access privilege (true immutability) or that any alterations are tamper-evident. This can be accomplished by several means, including redundant off-site storage, serialization and digital signatures, and limited functionality media for assuring a high degree of confidence that the transaction logs have not been altered. Once initial systems are certified, auditing code changes; thorough regression testing would also reduce the risk from of insider manipulation to the logs.

IAL System Design Considerations

- *Custodial solutions: distributed storage of logs.* Various configurations for log custody can be devised to improve confidence that a log has not been altered. A simple model would send copies of logs to multiple off-site storage facilities, thus assuring duplicate original files and requiring a multi-party conspiracy to alter logs. An alternative with greater information security features would be to split transaction records into two or more pieces, with each piece sent to a different (or multiple) off-site location. In this variation, multiple parties would have knowledge that a particular record exists but the collaboration of all such parties would be required to reveal the contents of any given record. Also, if one party deletes, alters, or loses its piece, the related pieces at the other locations would provide the necessary evidence that something is amiss.

- *Serialization and digital signatures.* A primary goal of audit logs is to have a complete record of transactions, accompanied by an accurate date- and time-stamp for each. In the paper world, a standard tool for meeting this goal is to use a continuous roll of paper that logs each transaction sequentially at the time it occurs. The paper roll is "tamper evident," because any missing transaction is physically apparent from a gap in the paper roll.

  In the shift to computerized recordkeeping, there are techniques for essentially reproducing the functionality of the continuous roll of paper. Electronic records can be digitally date- and time-stamped, to assure the integrity of the stamped record. In addition, records can be serialized by a system-generated counter and then given a digital signature. Due to the nature of digital signatures, it will be evident if any tampering occurs to the information about the transaction or if the date or time has been altered.

- *Limited functionality hardware.* Another way to mimic the paper roll is to use a write-once, read-many (WORM) storage drive that is designed so that data cannot be altered once it is written to disc. The advantage of a WORM drive is that the technology is designed to prevent alterations once data is written. This technology is slower than other storage devices and thus may burden functionality of high transaction systems. One risk in using WORM drives is physical security–a WORM drive containing the accurate data might be replaced by a drive with altered data. The use of multiple, distributed storage facilities can mitigate this risk.

When audited logs are immutable and cannot be altered, there are additional advantages for deterrence and proof of policy or legal violations. With immutability, deterrence may be improved for all users of the system. The announcement that immutable audits are in place can send a strong signal that policy violations will indeed be permanently recorded. Immutability also creates deterrence against violations by systems administrators or those who are allied with systems administrators. An additional advantage of IALs, especially when stored off-site, is that the actions of inside and outside hackers are more likely to be logged, without the ability of the hacker to tamper with the logs. For similar reasons, detection and proof can be improved with immutable audits. Efforts by hackers or insiders to erase the logs are less likely to succeed, increasing the likelihood of detecting violations and enforcing the policies.

Immutability also increases the probative value of logs as evidence. If it can be shown that a particular log file

containing certain evidence was immutable—that is, could not be altered (or could not be altered without showing evidence of alteration)—then it will be of greater value for use in investigations and subsequent criminal, judicial, or other enforcement actions.

When information sharing and collaboration systems like the ISE employ IALs, it can be clearly determined what communications have occurred between parties. When one party makes a formal request for information, that request is discoverable years later. This knowledge may open the door to better collaboration as receiving parties may be more inclined to respond, and, in doing so, prove they have been forthcoming with relevant information.

The primary benefit of IALs—beyond the incremental improvements in deterring, detecting, and proving policy violations—is to increase the level of trust that persons outside the system can have that policy is being followed in system usage. Effective audits that are perceived as effective from the outside can deter and detect "browsing" by system users who are looking at records where they have no authorized purpose to be doing so. Access to the audit logs can be granted to trusted parties, such as an agency's Inspector General or the Government Accountability Office, which can assess compliance with information sharing and privacy guidelines as well as with a system's stated policies. Even for classified systems, unclassified versions of reports can be made public that describe the extent of compliance with stated policies.

IALs may also help increase trust between information sharing parties, especially in areas where levels of trust have historically been low, for example, information sharing between federal law enforcement and state/local law enforcement. IALs can also improve trust and increase cooperation between the Federal Bureau of Investigation (FBI), and the Central Intelligence Agency (CIA); improve communications between incumbent agencies and newer organizations like the Department of Homeland Security and the Office of the Director of National Intelligence (ODNI); and help better integrate stakeholders that have not traditionally been part of the national security apparatus, such as the Department of Health and Human Services and the private sector. IALs that prove how information was accessed, by whom, and when, may lessen concerns.

B. Deciding what to log

When implementing IALs, initial decisions must be made as to what to log and how long to maintain records.

What is logged will be influenced by the need to satisfy oversight requirements.[1] In the face of extensive oversight requirements, one could envision an IAL system that would record all activity within a system. Logging all system activity would involve making a record of all information created, altered, and deleted by users; all information exchanged between systems; and all other information transactions that take place, including user queries, automated system updates, and database maintenance processing. System designers must also decide what level of granularity to record. A system might log at the level of individual records, for example, the entire file about a particular individual; or it might record at a field or cell level, for example, logging that the analyst viewed only a name and address field but not a Social Security number. Finally, a decision must be made regarding how long data should be retained—for example, whether data should be retained beyond the 30–year period required for declassification of foreign policy records under U.S. law.[2]

Designers of the ISE will need to consider the wide range of information that can potentially be logged. Such information includes:

- *User supplied data.* Users often supply systems with new information, for example, by adding or modifying a record. IALs, in systems designed for user input, will typically record all user modifications (i.e., additions, changes, and deletions).

- *Information exchanges between systems.* IALs can also be used to record information flows between systems. For example, an IAL might log when records were received or updated from other systems, and when records from the system being logged are published to secondary systems. Logging of these system-to-system flows will become more necessary as information is tethered between systems to its original source in order to improve currency or enable consistency of shared information. Using IALs to log such flows would be useful where definitive proof may be needed to show whether a record existed at a certain point in time or whether the most up-to-date information was used.[3]

- *User queries.* A common use of IALs may be to create an audit trail of what queries were made by which users,

[1] An organization might decide "what to log" based on meeting requirements in law. For example, in the private sector, corporations may decide what to log based on requirements in the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Financial Services Modernization Act of 1999 (also known as the Gramm-Leach-Bliley Act), or the Sarbanes-Oxley Act of 2002. They may also log in order to conform to industry best practices (and thus avoid liability for negligent practices).

[2] 22 U.S.C. § 4354.

[3] In large-scale systems with high transactions volumes, it may be too expensive to log all information flows. Nonetheless, long-term trends toward cheaper storage and transmission will make more detailed auditing feasible over time in a greater range of applications.

and when—for example, Eric Employee's access to the records of Sarah Suspect on June 1. In addition to the query itself, the system might log all records returned, that is, it could record the complete candidate list created in response to Eric Employee's initial query. In the example, suppose that the system presented 25 possible matches to Eric. The returns might have included, for instance, all matches including those records with small variations in the spelling of the name. From the returned list of 25 names, Eric may then select one or more of these candidates in an attempt to locate the correct Sarah Suspect. A policy and design issue is whether the system records only the query made by Eric Employee, the possible candidates presented to Eric, any records Eric selected from the candidate list (such as those about Sarah Suspect), or all of these. The decision to log all returns may be appropriate in systems or applications where collateral disclosure of personal information is a particular concern.[4]

- *Automated system updates and database maintenance processing.* Information systems often have automated processes that run periodically to keep the system operational. For example, system-wide updates are often used to purge expired records, to compute and store monthly-use statistics, or to apply external data enhancement (for example, to correct addresses that have been assigned new postal codes). If oversight in a particular system requires proof of the database state at any given point in time, the two options are to engineer such a system from the ground up,[5] or else to log all system-wide activity (e.g., use an IAL).

C. IALs may introduce new vulnerabilities

Depending on what is logged and how long it is retained, IALs have the potential to become comprehensive data collections. If, for example, IALs recorded all system activity and accumulated records of all transactions—inputs, queries, and returned data—the IAL itself may eventually contain more information than the original database or system that it logs. Containing everything within the original system plus records on the activities and interactions with and within the original system, the IALs could end up eclipsing the size of the underlying data sets. IALs may thus actually increase the possibility for (and possible negative consequence of) misuse. Given that potential, careful design and implementation are required so that IALs do not inadvertently create greater oversight and security challenges than they are intended to remedy in the first place.

This section discusses what protections might mitigate this secondary effect.

It is important to note that an overall audit system will likely include a variety of logging activities, only some of which would sensibly be done with an IAL. For example, user query activity might be logged to an analytic process that is designed specifically to detect atypical user behavior. User queries might also be logged in a manner to enable enterprise awareness, such as where two users show an interest in the same types of information. In such cases, the users could be notified, promoting collaboration in ways not previously possible. These mission-specific logging functions would need only a small subset of the data in the IALs, and they would likely not have the long data retention requirements of IALs.

IAL systems should have special features to mitigate the secondary effects of unintended use or disclosure of data through access to the IALs themselves. Because IALs potentially are so comprehensive, there is reason for caution in collateral (that is, non-audit or oversight) use of the IAL systems. The following features should be considered:

- *Record level encryption and shared keys.* One method to protect the IALs from unintended disclosure and potential secondary misuse is to restrict access to log records by requiring agreement among multiple parties before access is granted. Cryptographers have developed methods of shared keys so that data can be encrypted in a way that requires multiple keys for decryption (and thus access). These keys can be distributed among multiple parties, thus requiring their cooperation to gain access to any record and preventing any individual party—e.g. a systems administrator—from gaining access in order to uncover information or to alter logs. Ideally, each record would have its own unique set of shared keys to avoid reuse of keys on additional records.[6]

- *Custody of keys should be based on particular systems needs and how oversight trust is to be allocated.* For example, where appropriate in a particular application or with especially sensitive data, shared keys might be kept with a court and used only with a court order. In other cases, keys may be subject only to administrative, executive, or other procedural controls.[7] Key management issues

[4] For example, returns may include added identifiers (i.e., secondary identification criteria) such as date of birth, tax identity number, and last known address, which help the user quickly narrow down a large candidate list.

[5] There are numerous examples in the private sector in which organizations are required to be able to reconstruct what information was known when. For example, the Fair Credit Reporting Act requires that credit bureaus be able to reconstruct what information was in a particular credit file on any given day, and the Securities Act of 1934 requires that financial service firms be able to reconstruct account status or trading history at any particular time.

[6] In systems with significant transaction volume, key management might become unmanageable. One option might be to compute the encryption/decryption keys based on an algorithm controlled by a third party. Another strategy would be to uniquely encrypt groups of records, such as in chunks of 1,000 records.

[7] For example, keys might be held by Privacy Officers or Inspectors General within agencies, or external oversight agencies such as the

(how keys are created, distributed, and managed) are policy matters beyond the scope of this paper.

- *Use restrictions.* Because of their comprehensive nature and the potential for secondary abuse, access to IALs should be restricted from casual use. Even without policy constraints on access, the IAL systems described in this paper are also likely to be ill-suited for casual processing. IALs are an excellent tool, though, for showing that a particular transaction did or did not occur, and in what order, and thus useful for compliance auditing. They are also particularly well suited to long-term evidentiary tasks, such as proving years later whether a particular system activity occurred.

D. Other potential obstacles to adopting IALs

- *Institutional inertia.* It is not clear from existing literature why robust tamper-resistant audit logs have not been deployed in major government and private sector information systems. The Task Force and federal computer security documents such as the *Orange Book*[8] and the Common Criteria[9] have for some time called for effective audit mechanisms, but actual practice appears to lag considerably behind the aspirations. In considering how to implement IALs, additional attention may be needed to address institutional obstacles to deployment.

- *No developed market for IAL products, high cost.* With respect to IAL software, it would be ideal if competing organizations created, commercialized and commoditized IAL products, thus bringing to the market competitively priced options for organizations desiring such technology. With the ongoing drop in the cost of storage, processing, encryption, and transmission of data, the cost of new hardware is becoming increasingly affordable. To the extent that logging requirements become more widespread—either by legal requirements on the private sector or procurement decisions by government—it is likely that these functions will increasingly be built in to core products, thus reducing the costs significantly.

- *No obvious return on investment.* One institutional obstacle to adoption is that system owners do not necessarily perceive any measurable return on investment for funds spent on IALs. The intangible community benefits that may come from greater trust in the system are not directly measurable, and thus may not be factored into investment decisions by the operators or managers of such systems. To overcome investment disincentives, regulation or law could impose implementation of IALs. In such circumstances, care must be taken to legislate outcomes—that is, immutability—not specific technologies, as these may change, or different specific applications may require different technical solutions. The use of IALs may become more widespread without direct legislation if IALs become widely recognized as "best practice" for audit in response to existing record-keeping or certification requirements such as those in HIPAA, Gramm-Leach-Bliley, or Sarbanes-Oxley.

- *Incomplete assurance of trustworthiness.* IALs increase trust by assuring that activities in the system will be recorded and subject to after-the-fact verification. IALs do have inherent limitations, however, on both the input and output sides. On the input side, the logs will only record what is fed into the system. If system designers create a "back door" into the system, then secret access to the supposedly audited system may in fact occur. On the output side, IALs cannot establish what users do with the data once they have seen it. For instance, an analyst might speak on the telephone about the record, take a photograph of the computer screen, or memorize the information and write it down later. The assurance of trustworthiness provided by IALs, therefore, is less than complete because of the possibility that unauthorized access to data will occur through mechanisms that are not subject to the audit.

- *Decrease operational flexibility.* System managers are focused on achieving their organization's mission and are invariably under tight budgets and deadlines. As with security measures, implementation of IALs can be perceived to be in tension with more quickly implementing less secure system features. If the choice is between implementing a new feature in direct support of operations and delaying implementation to install robust logging, the former will usually win.

- *Negative impact on operational systems.* At least in the view of system managers, logging may get in the way of performance. An effective logging program

---

Office of Management and Budget might hold keys subject to release on meeting conditions in policy guidelines.

[8] Department of Defense Trusted Computer System Evaluation Criteria (DoD-5200.28-STD), first published in 1983, de facto standard for computer security

[9] See Common Criteria Project Sponsoring Organizations, "Common Criteria for Information Technology Security Evaluation, Version 2.1," (1999), http://csrc.nist.gov/cc/. This is the International Standards Organization information technology security process, including discussion of appropriate auditing.

may result in a drain on finite system resources. For example, consider a system that does not have enough spare processing cycles to invoke a log event for each employee query.

- *Resistance to oversight.* Another obstacle to deployment of IALs is resistance to oversight itself. The use of IALs may help assure outsiders that a system is being used in compliance with statutory or organizational policies. System administrators with high integrity—surely the vast majority of administrators—see little reason to spend scarce resources to prove that they are doing the honest job they know they are doing. For those few system administrators with low integrity, the incentive to avoid IALs is even stronger, because they would not wish to have wrongdoing in their domain detected.

- *Privacy of system users.* Strong auditing systems are likely to increase the granularity of surveillance on system users. The detail in audits might range from relatively high-level information, such as each query to a database, to relatively detailed information, such as all information flows and keystroke logging of each employee's use. As auditing occurs at a greater level of detail, the privacy of system users declines. While one might expect users of national security systems to have a low expectation of privacy (intelligence officials have no expectation of privacy and are frequently reminded of it; stickers on "outside" phones in their offices remind callers that their phone calls are being monitored), widespread audits of system use may have a deterrent effect on use of the ISE by national and homeland security officials.

- *Unintended disclosure or attack.* As noted above, IALs have the potential over time to eclipse the databases and information systems that they monitor. By recording all changes and user activity the logs themselves become formidable information repositories that may be subject to inadvertent disclosures or intentional attack. This paper has suggested that record-level encryption, shared keys, and distributed data sets can help mitigate insider abuse. These same features can help reduce the risk of inadvertent disclosure or intentional attack; nonetheless, information security in IALs is a significant issue that needs to be addressed in systems and policy design.

Policy Recommendations

There is significant promise in using IALs within an overall oversight and audit framework, particularly when applied to non-transparent information sharing systems like the ISE. The analysis in this paper suggests that IALs will be valuable in environments like the ISE with:

- High needs for deterring, detecting, and proving violations of policy and law
- High needs for protecting against insider threats from users with administrative privileges (or from those who control them)
- High needs to assure those outside the system that policy and law are being followed by insiders

To promote the successful implementation of IALs within the ISE, the Task Force believes the following recommendations should be pursued:

- *Use incentives or mandates to promote implementation of IALs.* The adoption of IALs faces institutional obstacles, including the lack of an obvious return on investment to system owners, and the possible reluctance of system administrators to subject themselves to such strict oversight. Where possible, procurement and other incentives should be used. Where necessary, because of institutional impediments or disincentives, mandates should be considered. When mandates are imposed, care should be given to specifying desired outcomes rather than demanding particular technologies or features.

- *Implement a staged plan for spreading deployment of IALs.* The program manager for the ISE within the Office of the Director of National Intelligence (ODNI) should, in coordination with individual agency chief information officers and other relevant officials, identify pilots for using IALs within information systems that are part of the ISE. In general, projects should be developed that encourage widespread experimentation and adoption of IAL systems. As lessons are learned from pilots, a plan should be developed to use IALs widely within the ISE. When implementing IALs, it is important to recognize that security and information assurance will be more effective to the extent that it is designed directly into every element of the network, as opposed to being retrofitted onto the system.

- *Audit the auditors.* In an approach described in this paper, the IALs would be stored at the record level in encrypted form, with strict procedures governing the unlocking of each encrypted record. If system use were audited, selected IAL records would need to be decrypted. Conducting oversight over the audit process would require an accounting of what IAL records were opened, by whom, and when. Such auditing would increase the confidence

of those outside the system that the IALs themselves are not being used in unauthorized ways. For those who favor more intensive use of audit logs, the need to audit the auditors is even greater.

Conclusion

In order to be effective, these policy recommendations need to be applied in a comprehensive manner. A piecemeal or selective implementation will not be sufficient to overcome the institutional and technical hurdles we have seen in this paper. In particular, the best incentives and implementation strategies will fall short if trust is not established through effective oversight and audit. Ultimately, the ISE's success rests on the extent to which the system is trusted by the public, policymakers and the users. IALs are a critical—if not exclusive—oversight component. Their successful implementation—and, by extension, the policy recommendations of this paper—can therefore be seen as the building blocks for greater innovation, information sharing, and efficiency within government.

Selected Bibliography

Bellare, Mihir and Bennet S. Yeey. "Forward Integrity for Secure Audit Logs" (1997). http://www.loganalysis.org/sections/research/fi.pdf.

Camp, Jean and J.D. Tygar. "Providing Auditing While Protecting Privacy" (1994). http://www.ljean.org/files/counting.html.

Common Criteria Project Sponsoring Organizations. "Common Criteria for Information Technology Security Evaluation, Version 2.1" (1999). http://csrc.nist.gov/cc/

Dempsey, James X. and Paul Rosenzweig. "Technologies that can Protect Privacy as Information is Shared to Combat Terrorism." Legal Memorandum 11. Heritage Foundation (2004). http://www.heritage.org/Research/HomelandDefense/lm11.cfm.

Department of Defense, Computer Security Center. *Orange Book*. Trusted computer system evaluation criteria (1985).

Golle, Philippe. "Protecting Privacy in Terrorist Tracking Applications" (2004). http://www.cfp2004.org/program/materials/w-golle.ppt.

Jonietz, Erika. "Total Information Overload." *Technology Review* (July 12, 2003). http://www.technologyreview.com/articles/03/07/impact0703.asp?p=3.

Kenneally, Erin. "The Legal Realities of Logs" (2004). http://www.sensage.com/about/releases/LegalRealities_Article.pdf.

Markle Foundation Task Force on National Security in the Information Age. "Creating a Trusted Network for Homeland Security" (2003). http://www.markle.org/markle_programs/policy_for_a_networked_society/national_security/projects/taskforce_national_security.php#report1.

Mercuri, Rebecca T. "On Auditing Audit Trails." *Communications of the ACM* 46: 1 (January 2003): 17-20.

Peha, Jon M. "Electronic Commerce with Verifiable Audit Trails" (1999). http://www.isoc.org/inet99/proceedings/1h/1h_1.htm.

Swire, Peter P. "Financial Privacy and the Theory of High-Tech Government Surveillance." *Washington University Law Quarterly* 77 (1999): 461-512. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=133340.

Technology and Privacy Advisory Committee. "Safeguarding Privacy in the Fight Against Terrorism." Department of Defense (2004). http://www.securitymanagement.com/library/TAPAC_Report0804.pdf.

Tygar, J. D. and Bennet Yee. "Dyad: A System for Using Physically Secure Coprocessors" (2002). http://www.cni.org/docs/ima.ip-workshop/Tygar.Yee.html.

MARKLE FOUNDATION

Markle Foundation
10 Rockefeller Plaza
16th Floor
New York, NY 10020-1903
Tel: 212/713-7600
Fax: 212/765-9690
www.markle.org