Control of Sensitive Information

Policy, Procedure, and Practice in a National Security Context

Duane Lindner*
Winalee Carter*

Introduction

Each of us lives and works in environments in which we have access to sensitive information. That information can range from personal financial information to legal information to information about personnel matters to details about intellectual property and on and on. There is a web of law, policy, procedure, and practice that governs how we manage such information—how we control access to it, how we protect it, how we share it. Formal and informal methods help establish and reinforce approaches to sensitive information management—what we control, how rigorous that control is, and how we react should we inadvertently lose control of such information. Frequently, our personal sensitive information management processes and practices become ingrained and we become relatively unaware of them, especially for those that are simply "common sense" or obvious practices. The risk/benefit analysis of posting our credit card numbers on line is easy to do. In other cases, policy (and training) helps reinforce the importance of sensitive information management—protection of commercially valuable information is underscored by institutional policy but reinforced by an understanding of the monetary value of such information—and by an awareness of what competitors could do with such information. Laws, policies, and procedures create a framework for management of sensitive information. Training and situational awareness—especially awareness of risk—help create an environment that establishes norms and practices for assessing sensitivity of specific information and for managing it.

For those of us who deal routinely with information that has national security implications, law and policy establish a comparatively rigorous framework for information management—a framework that establishes approaches to assessing the sensitivity of specific information; a framework that establishes policy and procedure for managing sensitive information. While such a framework is important, even critical; ultimately, management of national security information relies upon individual action and so information security relies upon establishing an environment where individuals make the right decisions, where they are equipped to make the necessary risk/benefit assessments regarding information control and supported by resources where they can seek advice and the information needed to make decisions. In organizations that deal with sensitive national security information, we ensure that we fulfill the requirements of law and the dictates of policy. But, we also explicitly attempt to create and re-

* Sandia National Laboratories

Sandia National Laboratories is a multi-program laboratory managed on operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

enforce a culture in which our staff are equipped to make appropriate decisions as they handle and manage sensitive information.

We will describe both the formal and informal procedures and practices that are used in a national security laboratory to manage sensitive information. We will also attempt to describe how information management practices in a relatively controlled environment might inform options for sensitive information management in more open institutions.

Frameworks for Management of Sensitive Information

Classified Information

Under statute and Executive Order, certain categories of information in government possession can be classified and therefore controlled according to the category and level of classification Current classification categories are: National Security Information, controlled under Presidential Executive Order and Restricted Data and Formerly Restricted Data, both controlled under the Atomic Energy Act. Levels of classification include Confidential ("undue damage to national security"), Secret ("serious damage"), and Top Secret ("exceptionally grave damage"), but these levels are only part of the story. Information at any level can be subject to additional controls under various caveats (e.g. NOFORN, Sigma, Compartmentalized Information, etc.) that limit access to groups with specific clearances, credentials, or "Need to Know". Statute and implementing policy govern generation, marking, protection, and distribution of classified information as well as impose strict requirements on those who produce and handle such information—accompanied by potential severe penalties for mishandling such information, whether intentional or unintentional.

Controlled Unclassified Information

In 2009, President Obama commissioned an interagency Task Force (led by the Department of Homeland Security and the Justice Department) with developing a standardized framework for management of Controlled Unclassified Information (CUI), a generic term for sensitive information that does not meets the legal or regulatory standards for classification (another term for such information that is widely used is Sensitive but Unclassified (SBU)). The task force recommended a definition for CUI:

> "*All unclassified information for which, pursuant to statute, regulation, or departmental or agency policy, there is a compelling requirement for safeguarding and/or dissemination controls*."

The task force attempted to identify all designations for CUI information across government. They catalogued well over one hundred, including such designations as For Official Use Only

(FOUO), Sensitive Security Information (SSI), CRADA Protected Information, Personally Identifiable Information (PII), and so on. The Task Force produced recommendations pertaining to management of such information in an attempt to simplify and regularize procedures across government. In their final report, they made 40 different recommendations, few of which have been fully implemented. As a result, management of CUI is subject to local procedures which vary from agency to agency and from institution to institution.

Obviously, every organization inside and outside of government possesses and manages information that can be described within the CUI definition.

It is important to note that requirements for control of information labeled CUI can be variously derived from "*statute, regulation, or … policy".* This heterogeneity of requirements and the large number of CUI types can create an extremely complex information management regime. At Sandia National Laboratories, we manage this complexity via generalized policies and procedures within an overall management framework but allow for specialized practices where necessary (e.g. management of medical records.)

Processes and Practices for Management of Sensitive Information

Determination of Information Sensitivity

Who determines if a specific piece of information is classified? At what level? With which caveats? In large part, this is the role of a small number of Original Classifiers with input from qualified individuals. With the oversight of Original Classifiers, committees of SMEs prepare Classification Guidance documents that provide details and specific guidance within topical areas. Many people (mostly professional staff) are trained as Derivative Classifiers (DCs)-individuals who are qualified to classify specific documents[*] based upon the Classification Guidance. But ultimately, the guidance is based on an assessment of risk (explicit in the definitions of the levels Confidential, Secret, and Top Secret). This is important because no guidance can possibly be comprehensive—the committees cannot anticipate everything that might create national security concerns within a topical area. This is especially true in areas such as biotechnology where the timeframe at which new discoveries and applications are occurring is much, much shorter than that of committee decision and vetting process. As a result, derivative classification can require an informed assessment of risk for specific information and circumstances—within the context of the guidance. A flexible, well constructed guidance is based on criteria that drive risk (this is not as important for guidance covering very specific technologies, devices, or projects—especially comparatively static instances).

For CUI, processes for identification of sensitive information are frequently not nearly so prescribed—although it is important to be aware of the heterogeneity of CUI regulations (e.g., specific law and regulation governs medical records). So here, reliance on trained and qualified

[*] In this paper, the word "document" as in "classified document" should be considered to be inclusive of all types of information: paper documents, computer files, images, spreadsheets, drawings, artifacts, etc.

staff and management is vital, as they typically determine sensitivities of information that they produce or acquire.

Marking

Procedures require that documents determined to contain sensitive information be clearly identified as such. Markings include (as appropriate) classification level and category, applicable caveats, CUI category, references to supporting regulation or other authority that supports designations, etc. Typically, sensitive documents also require use of cover sheets that incorporate highly visible indicators (colors, labels, graphics) of information sensitivities. This practice strongly reinforces a culture of awareness in sensitive information management.

Review

Any document slated for limited (e.g. proposals) or unlimited release (e.g. journal publication) is subject to various layers of review designed to ensure proper classification (and therefore marking and handling). Review also includes assessment to ensure CUI has been identified. Particular attention is focused on certain types of CUI, including commercially valuable information, export controlled information, and others. At Sandia, both staff and management have a strong desire to ensure that results of lab R&D is published as broadly as possible, so one function of document review for unlimited release is identification of ways to carefully edit documents to facilitate maximum information release while minimizing risks resulting from such release.

Control

Sensitive information is subject to strict modes of control. Rules govern how such information is stored, handled, and transmitted. Classified information is typically stored in safes, vaults, or vault-type rooms. Specific features required for storage facilities are governed by the classification level and category of documents to be stored. Storage of CUI is much less rigorous, but storage in locked cabinets and rooms is usually required. Restrictions on where and how sensitive material can be handled are tied to level of sensitivity and handling can be limited to Sensitive Compartmentalized Information Facilities (SCIFs) to Limited Areas, or to Property Protection Areas. Storage and handling of sensitive computer files are under analogous restrictions—computer networks at various levels of security are used as appropriate. Various networks are carefully isolated from each other, including by electronic isolation and by control of movement of recordable media. Access to such networks is also tightly controlled. Information protection hygiene requires that prior to review, documents in preparation be controlled and handled at the highest level of protection likely to be needed. Transmission of sensitive information is similarly regulated according to level and category, with requirements ranging from transmission via secure networks or channels down to use of encryption to move certain CUI on open networks.

Mistakes and Mistake-proofing

Control of sensitive information involves respecting a wide range of rules and restrictions. The complexity of the system is such that mistakes can and do happen. Information is mismarked

(or unmarked), safes are inadvertently not appropriately secured, computer records end up on networks that are less secure than prescribed, etc.

To help minimize mistakes, engineering controls and operational procedures help reduce possibility that human error creates problems. For example, human monitors double check locks to ensure that safes and vaults have been properly secured at the end of the day; electronic monitors provide a further layer of verification. Physical security in other forms is part of mistake proofing, as is document review.

Reporting (and self-reporting) are of key importance in identifying mistakes and mitigating consequences of mistakes. Establishing and sustaining a culture in which individuals promptly call attention to situations where oversight, mistake, or accident has led to a failure to properly control sensitive information supports an effective response to help minimize or eliminate potential negative consequences.

Clearances and Qualifications

Classification levels and identified sensitivities characterizing information are obviously essential, but just as important is a determination as to who has the ability to access such information. To access classified information, one must have an appropriate security clearance. Various types are clearance exist; different types qualify one to access classified information of different categories and at different levels. To obtain security clearances, individuals are subject to background investigations both to obtain the clearance and to maintain it. Different clearance types involve investigations of differing rigor (and invasiveness) and qualifications for higher levels of clearance are stricter than those for lower levels.

Access to CUI is much less formal, although controls can and do exist. These controls are based on such things as personal characteristics (e.g. to access Export Controlled information, one must be a US Person) or function (SSI access is limited to those in appropriate security or law enforcement roles).

The Need-to-Know Principle (NTK)

Appropriate clearance or other qualifications allow access, but do not mandate access to specific sensitive information. Ultimately, access is controlled by Need to Know. The NTK principle limits access to those who actually must have access to perform their job. NTK is applicable in controlling access to all types of sensitive information. Establishing NTK can be quite formal or it can be relatively informal. Ultimately, NTK establishes a significant requirement on those who possess sensitive information.

Formal processes to manage NTK can involve the establishment of NTK groups. Access to such a group may require special approvals, specific training, a formal briefing, or satisfying other requirements. Those possessing information subject to formal NTK controls are obligated to check that anyone receiving access to such information is in the governing NTK group.

More generally though, the NTK obligation requires anyone who is in possession of sensitive information ensure that recipients are both qualified to receive the information and require access to that information to perform their jobs.

Environment and Culture

Training

To effectively identify and manage sensitive information, individuals must be aware of what information is sensitive and why it is sensitive. They must also have a firm understanding of the policies, rules, and procedures in place to help effectively manage such information. This requires ongoing training and education. At Sandia, almost every employee will encounter some form of sensitive information[*] so training begins on the first day of employment. Training varies from general security awareness to specific training on procedures or types of sensitive information. Management establishes training requirements for each individual beyond the general requirements applied to all personnel.

A challenge in conducting such training is to ensure it remains relevant and does not foster rote repetition and complacency.

Awareness

Ongoing efforts keep personnel sensitized as to the importance of information management take many forms. Recurring communication via many different channels serves to remind everyone of the importance of this objective. Discussions of issues and "lessons learned" from lapses are routine at Department and Group meetings (with details that might reveal personnel information not included).

In addition, employees need to be aware of threats to information security. Information about publicly disclosed espionage activities targeting other institutions and government is routinely shared.

Work at Sandia is directed at protecting our own information and systems as well as that of other government entities. Insights into security issues surrounding protection of such systems is widely shared with personnel at appropriate levels of detail.[†]

Support

Efforts to manage sensitive information will inevitably lead to questions and a need or desire for additional insight. Since management of classified information requires high rigor and specific processes, institutions that deal with such information by necessity establish capabilities that can support both management and other personnel as questions arise. Information management specialists and qualified derivative classifiers comprise part of that support capability.

---

[*] While Sandia is extensively engaged in classified work, most Sandia employees are not involved routinely in such work. However, a majority of employees do encounter CUI in performing their duties.

[†] Briefings on how to conduct a "perfect heist" and results of a study on human factors involved in "phishing" attacks via email have been particularly popular.
J.L. Lafleur, L. K. Purvis, A. W. Roesler, and P. Westland, **The Perfect Heist**, Sandia Report, SAND2014-1790, March 2015.

Informed Risk Assessment

Accurate risk/benefit assessment requires an appropriate assessment of risk. In most environments, fairly accurate assessment of benefit is comparatively easy. An assessment of risk can be much harder. Part of the difficulty is that natural enthusiasm about the benefit of specific work can lead to amplification, while lack of specific information about risk—information about actions by adversaries or careful and thoughtful assessment of potential negative consequences—can lead one to minimize or discount risk. This is especially challenging since this latter information can be classified, sometimes at very high levels.

At institutions where individuals have access to this such information, a more realistic risk/benefit analysis is possible. Even if all participants in specific work cannot access full details, knowledge can help engender a culture of caution as appropriate.

Summary

Concerns regarding both public health and national security underscore information management concerns in biological R&D. The vast majority of work in this domain is holds great potential for positive benefit in each of these domains, promising significant benefits to human health and tools to improve national biodefense. Therefore, methods to enable broad information sharing while implementing methods to help minimize risk associated with disseminating information should be the objective. This situation is particularly challenging as a result of the rapid pace of discovery and technological change in biotechnology which can affect the risk/benefit calculus in sudden and discontinuous ways.

Approaches to help facilitate meeting this objective include tying information guidance to risk—with articulation of risk drivers, to facilitate understanding and decision-making in a changing environment. Policy and procedure must be part of any sensitive information management system but such controls are of limited value absent a suitable information management culture. All institutions have policy, procedures, and cultures that control sensitive information of other types—might it be possible to build on those structures to help manage information involving DURC? Training can ensure that personnel are can understand why information is sensitive, how to identify sensitive information, and what policies and procedures should be followed. Availability of resources to support information management are also important. But attention to establishing a culture that is aware of the risks and ready to help manage them is essential.

Accurate (or as accurate as possible) risk/benefit analysis can be very powerful in helping establish an information security culture, but access to important risk information is challenging in open environments.