Essential Elements of a Compliance Program

24 June 2016

Office of the Director of Compliance
National Security Agency
9800 Savage Road
Fort George G. Meade, Maryland 20755

ESSENTIAL ELEMENTS OF A COMPLIANCE PROGRAM

PURPOSE

This paper outlines a framework that can be used to develop an effective compliance program. It describes the essential elements of a compliance program along with a summary of how each is applied at the National Security Agency (NSA). This outline is based on NSA's research and more than six years of experience in developing and implementing NSA's Comprehensive Mission Compliance Program (CMCP).

BACKGROUND

The missions of NSA are protecting U.S. national security systems and producing foreign signals intelligence information. NSA must execute these missions in a lawful manner. Failing to carry out its missions in accordance with established law and policy could violate the rights of U.S. persons and harm national security, as well as result in the loss of authorities and the erosion of public trust. For these reasons, mission compliance has long been a part of the NSA culture.

NSA's analysis of best practices and criteria from the private and public sectors resulted in the development of an internal mission compliance program based on eight essential elements. The implementation of that program provides reasonable assurance that NSA activities remain consistent with law and policy.

In early 2016, NSA launched a comprehensive campaign – NSA in the 21st Century (NSA21) – a two-year plan to position the Agency to meet the increasingly complicated challenges of the future. It comprises two integrated and mutually reinforcing elements, a set of campaign initiatives and a corresponding organizational redesign, built upon the foundational themes of people, integration, and innovation. Through NSA21, the Agency will continue to enhance its internal mission compliance program.

EIGHT ESSENTIAL ELEMENTS

Here are the eight essential elements and details about NSA's implementation of them to date.

Element 1: Demonstrated Leadership Commitment

Organizational leaders demonstrate a commitment to developing and implementing an effective compliance program.

Building a robust and successful compliance program starts with an organization's leaders. The Society of Corporate Compliance and Ethics emphasizes this critical element in its book Compliance 101, updated in 2015 by authors Debbie Troklus and Sheryl Vacca.

> "Compliance begins with the top tier of the organization. Support from the top is very important; there can be no program at all, much less an effective one, without the vision and guidance of the board. It is the board that officially recognizes the need for a compliance program and authorizes its launch and implementation, including the hiring of a compliance officer. The first step toward implementation of a compliance program is management's communication of their commitment."

Within NSA, the Director is ultimately responsible for compliance. Key senior executives have been appointed to lead and shape the compliance framework on his behalf. In addition to the NSA Office of the Director of Compliance (ODOC), which manages the overall compliance program, dedicated compliance organizations exist within the Information Assurance, Research, Signals Intelligence, and Technology Directorates, and the NSA/CSS Threat Operations Center. These are known as the Directorate Compliance Components (DCCs).

The Director has given sufficient authority to the Director of Compliance to coordinate and implement a mission compliance program. The Director of Compliance reports to the Deputy Director and is independent of mission, legal, and policy organizations. Furthermore, the Director of Compliance and the DCCs are involved in and consulted on relevant program management and strategic planning decisions.

The Director, Deputy Director, and the Senior Leadership Team are personally involved in furthering mission compliance at NSA, and communicate the importance of mission compliance to all levels of the workforce. Both the Director and Deputy Director have addressed the workforce at annual mission compliance conferences, and the Executive Director has co-hosted the annual Torchbearer Awards ceremony to honor achievement in the field of compliance.

Element 2: Integration into Strategic Mission

The compliance program is fully integrated into the organization's strategic mission and is provided with an appropriate level of resources.

An organization's compliance officer and his or her staff must be involved in, and consulted on, relevant program management and strategic planning decisions to make sure that compliance concerns are integrated into the organization's strategic mission. This allows the organization to successfully comply with legal and policy expectations and, per Compliance 101, to save on the future costs of compliance by:

- embedding quality into existing processes;
- centralizing common processes and controls;
- focusing on the corporate culture;
- improving information system processes (embedding compliance into technology);
- emphasizing training; and
- monitoring for compliance.

Furthermore, Troklus and Vacca emphasize that leaders must support the compliance program with an appropriate level of resources.

> "Resources and space cost money, and most organizations have limited, even diminishing resources. While the level of commitment is not necessarily correlated directly with the resources (human and financial) allocated, a responsible budget must be developed in consultation with the Compliance Officer. An organization unwilling to commit the necessary resources isn't demonstrating support for the compliance program and – unquestionably and unfortunately – that message too will filter down through the organization."

At NSA, compliance is integrated into the Agency's strategic mission. NSA's strategic plan includes a goal, entitled "Manifesting Principled Performance," that is directly related to mission compliance. It states, "Accomplishing our missions with a commitment to a principled and steadfast approach to performance through compliance, lawfulness, and protection of public trust must be paramount."

NSA has committed significant resources to manage and implement the mission compliance program. The Agency provides funding that aligns with the Director of Compliance's goals and is needed to develop and maintain the corporate compliance capabilities and processes. Additionally, more than 300 personnel across multiple directorates and organizations support the program.

Element 3: Management of Compliance Program and Resources

The organization competently manages the personnel, funding, and policies necessary for an effective and comprehensive compliance program.

An organization must commit sufficient funding and personnel resources to enable successful operation of the compliance program. According to compliance expert Martin Biegelman in his book Building a World-Class Compliance Program, this includes having "an adequate number of highly skilled people with appropriate authority to successfully carry out the compliance program mandate."

NSA has committed a significant number of personnel to manage and implement the mission compliance program. These personnel, including dedicated compliance officers, manage NSA's rules, plan and program funding for enterprise compliance activities, train personnel in concert with the NSA Office of General Counsel, develop and implement technical safeguards, and set up systems to monitor and guide NSA's activities.

The compliance program funds, managed by ODOC, enable successful mission compliance operations. ODOC, in coordination with the DCCs, plans and programs resources needed to develop and maintain corporate technical capabilities for compliance. Finally, NSA maintains up-to-date policies informing NSA employees of their mission compliance responsibilities and obligations.

Element 4: Rules Management, Compliance Standards, and Monitoring and Assessment of Compliance

The organization competently manages the rules, compliance standards, and monitoring of compliance.

Biegelman's work focuses on corporate compliance but his thoughts on managing rules and assessing compliance with them apply equally to government compliance efforts. He uses the Federal Sentencing

Guidelines for Organizations (FSGO) as an outline for building an effective compliance and ethics program.

> "Organizations must 'establish standards and procedures to prevent and detect criminal conduct' as well as ensure that organizational policies and procedures are followed. This includes standards of business conduct and internal controls reasonably capable of reducing the likelihood of criminal conduct and other violations of policy."
>
> "The FSGO require that organizations periodically evaluate the effectiveness of their compliance program and including monitoring and auditing systems designed to detect criminal conduct."

NSA has a corporate mission compliance rules management team. This team leads and advances processes to gather, organize, maintain, and provide access to the mission compliance rules contained in authorities, policy, and procedures.

NSA has established compliance standards that prescribe the internal control framework necessary to provide reasonable assurance of compliance with applicable laws, policies, and procedures, including those designed to protect U.S. person privacy during the conduct of mission operations. ODOC identifies where compliance standards are needed based on mission needs and ongoing risk assessments. Compliance standards may address mission functions within any of the main areas covered under various minimization procedures, and may also be developed for key mission-enabling processes that span mission functions.

NSA is increasingly leveraging technology to implement those standards throughout its compliance program, which allows it to augment – not wholly replace – human safeguards. The Agency uses technology to maintain the continuity of its external authorizations, from signed paperwork down to the bits and bytes. It also uses technology to record and review activities, making sure that laws and policies that guide NSA's operations are followed. Where appropriate, legal and policy guidance is embedded directly into the IT architecture. This is accomplished by developing and employing a suite of mission compliance services that are embedded or interact with tools, applications, and other components of the IT system to support and enhance the Agency's compliance posture.

Finally, monitoring and assessment personnel track and analyze key mission compliance metrics to ensure that internal controls are working as intended to inform leadership of potential problem areas and develop solutions.

Element 5: Awareness and Training

Employees are aware of compliance responsibilities, principles, and initiatives, and have sufficient training to conduct their jobs in a compliant manner.

Abigail Adams noted, "Learning is not attained by chance. It must be sought with ardour and attended to with diligence." This thought is echoed by multiple sources. According to Building a World-Class Compliance Program, "One of the most important elements of an effective compliance program is training for all employees from the CEO down. Appropriate training reinforces an organization's commitment to ethical conduct and compliance with policies, procedures, and laws."

NSA's compliance program personnel regularly communicate the importance of mission compliance, and provide effective training on relevant laws, policies, procedures, and safeguards to the workforce. NSA hosts an annual Mission Compliance Conference and other routine events and meetings that are designed to strengthen the compliance community and increase awareness of the compliance program.

NSA's National Cryptologic School has a robust compliance curriculum comprising more than 15 courses. All NSA personnel (civilians, military members, integrees, and contractors) are required to be familiar with and agree to uphold the laws, policies, procedures and regulations that govern NSA mission activities and implement privacy protections for U.S. persons. Government employees take regular training throughout their careers in order to ensure proper handling of U.S. person information.

- All employees are required to take annual core Intelligence Oversight training.
- Employees requiring access to raw SIGINT data under FISA and FISA Amendments Act (FAA) authorities are required to take additional annual training specific to FISA/FAA requirements.
- Employees may be required to take advanced training depending upon their assigned mission.

Element 6: Risk Assessment and Management

The compliance program is informed by identified risks, and high-risk areas receive additional scrutiny and attention.

As a fundamental component of an effective compliance program, risk assessment is designed to help leaders better understand the extent of risk exposures that could potentially result in loss of authority, credibility, or mission capability. Risk assessment is one of a number of tools that support management decisions, priorities, and resource allocations. The Committee of Sponsoring Organizations (COSO) of the Treadway Commission's paper, *Risk Assessment in Practice,* emphasizes this point.

> "Given that risk is integral to the pursuit of value, strategic-minded enterprises do not strive to eliminate risk or even to minimize it, a perspective that represents a critical change from the traditional view of risk as something to avoid. Rather, these enterprises seek to manage risk exposures across all parts of their organizations so that, at any given time, they incur just enough of the right kinds of risk – no more, no less – to effectively pursue strategic goals. This is the "sweet spot," or optimal risk-taking zone…."

At NSA, risk management officers within ODOC assess the potential risk of non-compliance with the rules designed to protect privacy in mission operations. These risk assessments balance the inherent risk of non-compliance against the level of mitigation. Inherent risk considers both likelihood and impact of non-compliance, while mitigation includes ongoing compliance activities that mitigate risk. These assessments, performed at least annually, help to drive CMCP resources and activities. Areas of higher risk receive additional scrutiny and attention.

Element 7: Incident Management

Compliance incidents are swiftly contained and investigated; and, appropriate corrective action is taken.

Upon reporting of a potential incident, compliance organizations must conduct compliance incident management activities by applying the relevant policy, authorities, and/or legal issues, taking corrective action, and responding to the needs of the organization's internal and external overseers. In addition, the program must identify the root cause and assess the impact of incidents to continuously inform the evolution of the compliance program. Building a World-Class Compliance Program recommends several relevant actions to consider in response to potential incidents of non-compliance, including:

- "Conduct a thorough and professional investigation of the incident."
- "Assess, redesign, and improve relevant internal controls to mitigate future occurrences."
- "Communication and training…to reinforce the entity's values, code of conduct, and expectations."

When a mission compliance concern is identified, NSA immediately stops any non-compliant activity, and takes appropriate corrective actions, including disciplinary actions when appropriate. The Agency uses a common corporate reporting tool to capture and track incidents of non-compliance. Events deemed to be egregious must be reported immediately upon recognition to the OIG.

Element 8: Effective Oversight

Compliance officials effectively collaborate with external overseers and conduct periodic self-assessments, along with independent review of the compliance program.

As noted in Compliance 101, "an effective compliance program is a process of constant evaluation. The key is to strive for and demonstrate a process for continually improving on compliance activities and evolving your compliance program and its activities."

NSA's compliance program and personnel frequently interact with, and are assessed by, internal and external oversight organizations, including: the NSA/CSS Inspector General, NSA/CSS Office of the General Counsel, Department of Justice, Department of Defense, Office of the Director of National Intelligence, Congress, the Privacy and Civil Liberties Oversight Board, and the Foreign Intelligence Surveillance Court.

NSA's internal compliance program is in addition to, and works in concert with, the broader Intelligence Oversight (IO) efforts that are driven by the Department of Defense. The IO program focuses on oversight (quarterly incident reporting) and certain specifically-required compliance activities such as training.

ODOC also conducts periodic self-assessments to include Compliance Vulnerability Discovery, an effort charged with performing outcomes-based activities to proactively discover compliance vulnerabilities. Compliance Vulnerability Discovery activities are centered on high-risk areas within NSA's Comprehensive Mission Compliance Program and afford ODOC the opportunity to focus tightly into areas of concern.

REFERENCES

Building a World-Class Compliance Program: Best Practices and Strategies for Success. Martin T. Biegelman; Daniel R. Biegelman. John Wiley & Sons, 2008.

Compliance 101: How to build and maintain an effective compliance and ethics program. Debbie Troklus, Sheryl Vacca. Society of Corporate Compliance and Ethics, 2015.

Risk Assessment in Practice, Deloitte & Touche, LLP, Patchin Curtis, Mark Carey. Committee of Sponsoring Organizations (COSO) of the Treadway Commission, May 2013.

RESOURCES

Arms Export Control Act and the International Traffic in Arms Regulations.

Compliance Management for Public, Private, or Nonprofit Organizations.

Equal Employment Opportunity Management Directive 715, Federal responsibilities under Section 717 of Title VII and Section 501 of the Rehabilitation Act.

Factors in Prosecution Decisions for Environmental Violations.

Federal Sentencing Guidelines for Organizations (FSGO).

Government Accounting Office (GAO) Standards for Internal Control in the Federal Government, September 2014.

Health Care Compliance Association, Evaluating and Improving a Compliance Program: A Resource for Health Care Board Members, Health Care Executives and Compliance Officers (2003).

Internal Control – Integrated Framework, Executive Summary, Committee of Sponsoring Organizations (COSO) of the Treadway Commission, May 2013.

International Organization for Standardization (ISO) 19600:2014, Compliance Management Systems—Guidelines

Organization for Economic Cooperation and Development Guidelines on the Protection of Privacy and Trans border Flows of Personal Data of 1980.

The Complete Compliance and Ethics Manual. Society of Corporate Compliance and Ethics, 2014.