Government Security Compliance

From 2015 to 2018, the United States Federal Government drastically reduced the number of estimated cyberattack incidents from 30,000 to only 125. How did they accomplish this? The Government established a set of rules and regulations called Government Security Compliance to improve security while also managing and maintaining cybersecurity costs.

Government Security Compliance defines the requirements that all government agencies and partnering private companies have to follow in order to improve security, protect data information, and not get penalized by Congress.

Cyber-Threats

Based on data analysis, there are two leading threats to the government's security.

Insider Threats

Insider threats are internal data breaches that are supported or initiated by a current government employee. These threats are easier to accomplish compared to external threats as the government employee already has access to the system and does not need to steal another employee's credentials.

An example of an inside threat is Edward Snowden's intelligence data breach from the Central Intelligence Agency. Snowden is infamous for leaking classified information from the CIA, and he has been charged with theft of government property and espionage.

Intentions aside, these insider threats tend to leave a worrying effect on Federal professional and administration employees who are unable to achieve objectives due to the fear that another insider threat may be around the corner.

External Threats

Although insider threats may be easier to accomplish, statistics show that more often government data breaches are a result of external threats. As time goes on and cybersecurity improves, external threats are becoming much more complicated and intimidating. However, these external threats start from a common baseline: stealing an employee's credentials in order to have access to the system.

Unfortunately, all hackers need to create a large data breach is just one employee's username and password. Even though employees are constantly instructed to add new characters to their passwords such as special characters, numbers, etc., hackers

using advanced persistent threats (APT) can steal user credentials to pass through the cyber defense and act as an employee.

Government Security Compliance

There is a major factor in government security compliance: FISMA, with assistance from NIST SP 800-53. Both work together to improve existing government cybersecurity initiatives and install new regulations that will further protect the government agency.

FISMA

The Federal Information Security Management Act (FISMA) requires federal agencies to develop, document, and implement an information security and protection program. Many federal agencies do not have a cybersecurity plan, and if they do, it is not active. FISMA strives to reduce the security risk to federal information and data and more importantly establish an active cybersecurity plan.

FISMA sets up six separate initiatives for a federal agency to be government security compliant.

- **Information System Inventory**
  Every federal agency is required to keep an inventory of all the information systems that are utilized within the organization. This defines what needs protection and what does not need protection. In a cybersecurity plan, this information seeks to protect active information systems and disregard inactive information systems. Additionally, if there are changes for any information system, the agency must report the integration. As a result, if an agency reactivates a previously inactive information system, the cybersecurity plan can incorporate the newly activated information system.
- **Risk Categorization**
  Each federal agency must categorize all information in order of risk to assure that sensitive information has the highest level of security. Risk categorization balances out the management of security required so that low-risk information only requires low-level security measures. This manages the amount of security required which balances the budget and maintains it to prevent overspending.
- **System Security Plan**
  FISMA requires agencies to create a security plan and constantly update it. As hackers are making efficient methods for stealing government data, agencies have to keep up with their competitors and be well prepared for any sudden and new types of attacks.
- **Security Controls**
  NIST SP 800-53 defines an extensive outline of security controls to be FISMA compliant.
- **Risk Assessments**
  NIST SP 800-30 outlines how agencies can conduct risk assessments to find issues within the agency.

- **Certification and Accreditation**
  FISMA requires officials to conduct annual security exams to ensure that the risks are at a minimum.

Benefits of FISMA
One benefit of being FISMA compliant is that private businesses can be associated with or attract potential partnerships with federal agencies. Additionally, being FISMA compliant assures greater security for both the federal agency and the private business that is associated with it.

Penalties of FISMA
If a federal agency is not FISMA compliant, there are several consequences. First, the agency receives a censure by Congress. Next, for the federal agency, they receive a reduction in federal funding. Lastly, that agency has reputational damage.

How Biometrics Can Help

Biometric authentication offers a solution to help federal agencies meet FISMA compliance requirements while reducing the risk of internal and external security threats.

Because most external threats deal with stealing user credentials, using a fingerprint as a password creates a huge gap between hackers and the agency.

Advanced Persistent Threats are unable to copy the several thousand pieces of data that a fingerprint contains.

BIO-key delivers biometric authentication solutions that have stood the test of time and our technology is trusted by the U.S. and international government agencies to authenticate and identify individuals. Government contractors rely on BIO-key to deliver a secure and compliant multifactor authentication solution.