NIST Standards

Posted by Mike Allerton, TCC IT Process Analyst

Background

The National Institute of Standards and Technology (NIST) was founded in 1901 with the intent of making U.S. commerce more competitive and trustworthy. In 2002, Congress signed the Electronic Government Act into law to improve the management of government information and services. As part of that Act, the Federal Information Security Management Act (FISMA) assigns NIST with the responsibility of establishing security recommendations for all government agencies and companies that do business with the government.

As a result, NIST published FIPS 200 *Minimum Security Requirements for Federal Information and Information Systems* which established and defined *families* of security control areas. NIST also published Special Publication 800-53 which is a catalog of administrative and technical controls within those families that should be instituted based on a given data set's security categorization. Most recently, this government department published a further refinement of these standards specifically focused on *Controlled Unclassified Information* (CUI), Special Publication 800-171. All contractors and subcontractors of the US government who handle sensitive federal information while assisting federal agencies accomplish their missions are subject to this new regulation.

Cyber security breaches are an all too common threat in today's business world. In February of this year, the Commission on the Theft of American Intellectual Property updated its original report with an estimation that the annual cost to the American economy exceeds $225 billion and could be as high as $600 billion. Not only are designs stolen, but counterfeit goods are produced and imported back into the U.S. The cost of trade secret theft is more difficult to estimate because companies might not even be aware that their intellectual property has been stolen, but is the majority of that annual cost.

If your company wants to do business with the government, it must be able to certify that it has responded to the complex and shadowy cyber environment. If your company has access to federal information systems or government data, as in sub-contractors of U.S. defense contractors for example, the data contained in your computer systems should be treated as restricted information and protected.

Compliance

NIST SP 800-171 provides a tailored, standardized set of mechanisms that non-federal organizations should consider and respond to, but they are not a set of regulations that must be followed. Each business must decide for itself how to solve their security issues. This was done on purpose -- there is guidance without mandates. There is no need to rip out mature solutions already in place, yet for those new to the issue, they provide the right questions to ask.

The first step toward compliance is a security assessment. Organizations can assess themselves; however, all assessments require comprehensive documentation exhibiting how the mechanisms are implemented and that they are working. In the assessment, you will cover 109 requirements spread over 14 families – with a couple other associated families.

The first element of each family is a coherent set of policies and procedures that every responsible person in your organization should be trained on and follow. The second element is the technical application of those procedures in system configurations and tools. With each of the requirements answered, you can assume a strong safeguarding of your data consistent with federal standards.

For more information on TCC's IT Managed Services, please visit our website https://www.e-tcc.com/managed-services.