Security Frameworks

Allan Wheelock

University of Advancing Technology

Author Note

This paper was prepared for NTS 435 International and Federal INFOSEC Standards and Regulations, taught by Joseph Pollock.

Security Frameworks

Perhaps one of the most important security frame works is FISMA, or the Federal Information Security Modernization Act. This framework was put in place by CISA, or the Cybersecurity and Infrastructure Security Agency. This framework was originally put into place in 2014. Since then, this framework has been updated annually.

The point of this framework was to update the Federal Government’s cybersecurity practices. There were three main ways that it did this. “Codifying Department of Homeland Security (DHS) authority to administer the implementation of information security policies for non-national security federal Executive Branch systems, including providing technical assistance and deploying technologies to such systems; Amending and clarifying the Office of Management and Budget's (OMB) oversight authority over federal agency information security practices; and by Requiring OMB to amend or revise OMB A-130 to "eliminate inefficient and wasteful reporting." (cisa.gov). This was a really important framework to put into place because it allowed CISA to inform the DHS on how to help other federal agencies on how to protect themselves in the cyber world.

In addition to assisting DHS on cybersecurity within their own organization, FISMA states that DHS can provide additional operational and technical assistance to civilian agencies working with various branches of the federal government. Another function of FISMA is that it puts the federal information security center under DHS law. Some of the revisions from the added versions were only around for a few years before they were taken off and are no longer used.

FISMA is an important security framework put into place by an important organization. CISA is the organization in charge of cybersecurity in the federal government. In addition to putting FISMA in place they are also responsible for protecting us from cyber threats. “We look at the entire threat picture and work with partners across government and industry to defend against today’s threats while securing the nation’s critical infrastructure against threats that are just over the horizon, “(cisa.gov). The CISA is a fairly new organization, founded only in 2018. One great thing about CISA is that they aren’t specific to the public government sector, but they also do work with the private sector. It’s a big ask for an organization to protect government and independent sectors from cyber threats.

Overall FISMA is a very important security framework and can be applied in many different fashions and organizations. With the power of FISMA and the work of CISA and the DHS, cyber space in the US is ensured to be safe.

References

Federal Information Security Modernization Act | CISA. (2022). Retrieved 27 January 2022, from <https://www.cisa.gov/federal-information-security-modernization-act>

ABOUT CISA | CISA. (2022). Retrieved 27 January 2022, from https://www.cisa.gov/about-cisa