Cybersecurity Standards, Policies, Guidelines, and Agencies

Standards

FIPS 201

201 FIPS 201 (Federal Information Processing Standard Publication 201) is a United States federal government standard that specifies Personal Identity Verification (PIV) requirements for Federal employees and contractors. FIPS 201 was developed to satisfy the technical requirements of HSPD-12, approved by the Secretary of Commerce, and issued on February 25, 2005.

FIPS 140-2

Federal Information Processing Standard (FIPS) Publication 140-2, (FIPS PUB 140-2),[1][2] is a U.S. government computer security standard used to accredit cryptographic modules. The National Institute of Standards and Technology (NIST) issued the FIPS 140 Publication Series to coordinate the requirements and standards for cryptography modules that include both hardware and software components.

NIST 800 53 Rev 4

In April, 2013, NIST published an update, Revision 4, to NIST Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organization. The guide was developed and is maintained by the Joint Task Force Transformation Initiative Interagency Working Group, part of an ongoing information security partnership among the U.S. Department of Defense, the Intelligence Community, the Committee on National Security Systems, the Department of Homeland Security, and U.S. federal civil agencies.
SP 800-53 Revision 4 has been updated to reflect the evolving technology and threat space. Example areas include issues particular to mobile and cloud computing; insider threats; applications security; supply chain risks; advanced persistent threat; and trustworthiness, assurance, and resilience of information systems.

ISO/IEC 27001:2013

(International Organization for Standardization and International Electrotechnical Commission) specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization.
It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization.

The requirements set out in ISO/IEC 27001:2013 are generic and are intended to be applicable to all organizations, regardless of type, size or nature.

ISO 17025

ISO/IEC 17025 was first issued in 1999 by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). It is the single most important standard for calibration and testing laboratories around the world. Laboratories that are accredited to this international standard have demonstrated that they are technically competent and able to produce precise and accurate test and/or calibration data.

Policies & Guidelines

National Critical Infrastructure Information Sharing and Analysis Centers (ISACs)- Presidential Directive 63- 2003

Information Sharing and Analysis Centers (ISACs) were created as a result of Presidential Decision Directive 63 (PDD-63) in 1998. The directive emphasized that, because 90% of the nation's critical infrastructures are owned and operated by the private sector, a public and private partnership is needed to share information about physical and cyber threats, vulnerabilities, and incidents to help protect the critical infrastructures of the United States. PDD-63 was updated in 2003 with Homeland Security Presidential Directive/HSPD-7 to reaffirm the partnership mission. Today there are thirteen ISACs for critical infrastructure including the Financial Services, Electric, Energy and Surface Transportation sectors.

Federal Systems (ATO) - Authorization to Operate

After completing a security assessment, the head of an agency (or their designee) can authorize the system for use, or grant an Authority to Operate (ATO). An agency grants an ATO according to a risk-based framework that analyzes how a vendor has implemented the security controls within their IT environment.

Federal IT Shared Services Strategy- 2010

The Federal 25 point implementation for IT shared services strategy covers the entire spectrum of IT shared service opportunities throughout the Federal Government and promotes the use of existing and new strategic sourcing methods where agencies can combine their buying power for similar IT needs and get lower prices and improved service leverage in the process of eliminating duplication and consolidate commodity IT systems, services, and related contracts in order to maximize the return on IT investments across the federal government and agencies. The Shared-First approach creates new opportunities for industry to provide shared IT services to agencies that are more agile in delivery and more responsive to a wide variety of evolving mission, support, and commodity IT requirements.

Federal Cloud First Policy- 2010

The Cloud First policy mandates that agencies take full advantage of cloud computing benefits to maximize capacity utilization, improve IT flexibility and responsiveness, and minimize cost.

The Cloud First mandate requires agencies to comply in moving services to the cloud. These cloud IT services provide convenient, on-demand access to a shared pool of computing resources that can be quickly and easily configured, provisioned, and released, including a "rent-not buy", commodity approach to procuring it services.

Federal Identity Credential and Access Management Program- (FICAM) Implementation Guidance Part B - 2011

In recent years, increasing emphasis has also been placed on improving the physical security of the hundreds of thousands of facilities that the Federal Government owns and leases to support the diverse mission work of its agencies and the need to develop a common framework that includes key practices for guiding agencies physical security efforts, such as employing a risk management approach to facility protection, leveraging advanced technology such as near real-time situational awareness using video, voice, and data, improving information sharing and coordination.

H.R. 1731 – National Cybersecurity Protection Advancement Act of 2015

(Sec. 2) Amends the Homeland Security Act of 2002 to allow the Department of Homeland Security's (DHS's) national cybersecurity and communications integration center (NCCIC) to include tribal governments, information sharing and analysis centers, and private entities among its non-federal representatives. (Sec. 3) Requires the NCCIC to be the lead federal civilian interface for multi-directional and cross-sector sharing of information related to cyber threat indicators, defensive measures, and cybersecurity risks for federal and non-federal entities.

EU Rules

The Safe Harbor Act was created to help US companies comply with EU privacy rules on its citizens. As a company if you collect and/or hold PII (personally identifiable information) on EU citizens you must comply with the EU rules for privacy which are much more strict than US rules and are also more tightly observed. The Safe Harbor Act, in essence, allowed US companies to sort of self-certify that they were in compliance. Most of the companies that were caught and determined not to be in compliance were identified when a consumer or another company complained.

The Ruling states that Safe Harbor is invalid. There is still much speculation as to how this impacts US companies and what they need to do to comply and avoid strict scrutiny and investigation. The ruling came about after the Snowden release of secrets which alleged that NSA had access to servers and data bases around the US, with an emphasis on large companies like Google and Facebook who may have been cooperating with NSA, thus allowing access to EU citizen data on US servers.

As far as the EU rules go, companies who use servers, for storage or otherwise, that are located in the EU, must be in compliance if they need to move data in and out of the EU even if that data is not that of an EU citizen. You may claim you hold no data on EU citizens, but that distinction will likely not matter when a complaint is made and may be very costly until a full investigation is completed.

Agency

NERC

NERC is a self-regulated organization. In June 2007, the U.S. Federal Energy Regulatory Commission (FERC) granted NERC the legal authority to enforce reliability standards with all users, owners and operators of the bulk power system in the United States.

Office of Management and Budget – OMB-M-11-11 - 2011

Presidential Mandate that each Federal agency use PIV credentials as the common means of authentication for access to that agency's facilities, networks, and information systems, to be effective in achieving the goals of HSPD-12 and realizing the benefits of PIV credentials.

For More Information:

www.psasecurity.com/education/cybersecurity

Source: http://www.psasecurity.com/education/cybersecurity

Resources: http://www.nist.gov/
http://www.nerc.com/Pages/default.aspx
https://www.whitehouse.gov/omb
https://ec.europa.eu/digital-agenda/en/cybersecurity
https://www.congress.gov/bill/114th-congress/house-bill/1731
http://www.idmanagement.gov/sites/default/files/documents/FICAM_Roadmap_and_Implementation_Guidance_v2%200_20111202_0.pdf
http://www.gsa.gov/portal/content/190333
https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/25-point-implementation-plan-to-reform-federal-it.pdf
http://www.isaccouncil.org/aboutus.html
https://www.fedramp.gov/faqs/what-is-an-authority-to-operate-ato/