Cybersecurity & the Federal Government

Our Nation's security and economic prosperity are vested in the fidelity and integrity of our Federal communications and information infrastructure. Cybersecurity threats represent our most significant challenges to the stability of the United States. As such, fortifying our Nation's cybersecurity has become one of our most critical initiatives.

Information Security & Data Protection

Our nation's data is at risk, and as a supplier to the US Government you are responsible for understanding and mitigating those risks. These responsibilities are articulated through the following means.

Executive Orders

An executive order is a directive by the president of the United States that manages operations of the federal government. The legal or constitutional basis for executive orders has multiple sources.

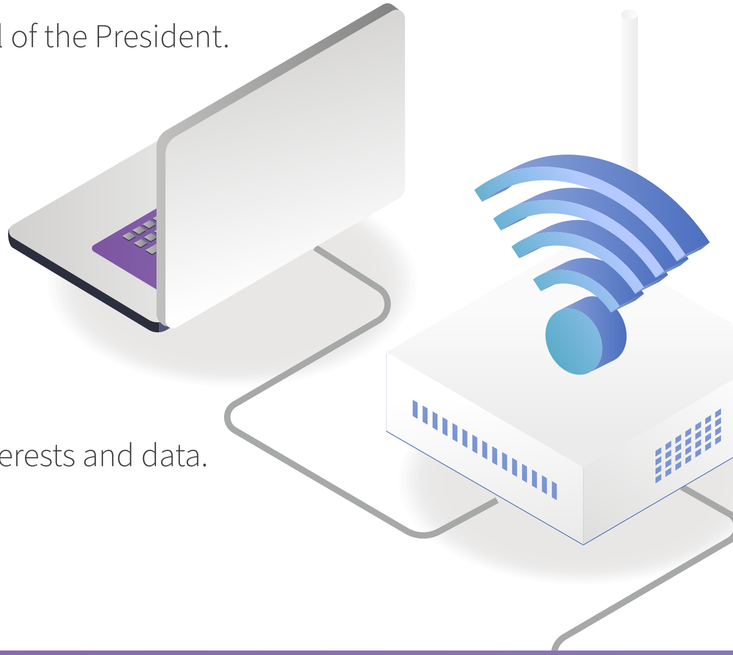
Federal Statutes

Federal statutes are the laws passed by Congress, usually with the approval of the President.

Federal Regulations

Federal regulations are issued by the various federal administrative agencies, which get their authority to regulate from specific statutes. Regulations are designed to implement and interpret statutes.

These components work collaboratively to assure the protection of U.S. interests and data.



Government data breaches pose one of the largest threats for US government entities in 2022 and beyond. As geopolitical tensions rise between Russia and the West, targeted cyber attacks against the federal, state, and local governments are increasingly likely. In fact, the FBI recently warned that ransomware is straining local government services, as local governments are favorite targets of hackers, second only to academic institutions.”

Source: https://www.govpilot.com/blog/government-data-breach-prevention-and-examples?

Information Security & Data Protection

Our nation's data is at risk, and as a supplier to the US Government you are responsible for understanding and mitigating those risks. These responsibilities are articulated through the following means.

Relevant Executive Orders, Legislation & Regulations

EO 13800 "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure"

EO 13873 "Securing the Information and Communications Technology and Services Supply Chain"

EO 14028 - "Improving the Nation's Cybersecurity"

32 CFR § 2002 "Controlled Unclassified Information"

48 CFR § 52.204-21 - Basic Safeguarding of Covered Contractor Information Systems

Federal Information Security Management Act (FISMA) 2014

DFARS 252.204-7008 "Safeguarding Covered Defense Information Controls"

DFARS 252.204-7009 "Limitations on the Use or Disclosure of Third- Party Contractor Reported Cyber Incident Information"

DFARS 252.204-7012 "Safeguarding Covered Defense Information and Cyber Incident Reporting"

DFARS 252.204-7019 "Notice of NIST SP 800-171 DoD Assessment Requirements"

DFARS 252.204-7020 "NIST SP 800-171 DoD Assessment Requirements"

Standards & Publications

DOD Instruction 5200.48 “Controlled Unclassified Information”

DOD Instruction 8500.01 “Cybersecurity”

DOD Instruction 8510.01 “Risk Management Framework for DoD Information Technology”

NIST SP 800-53 “Security and Privacy Controls for Information Systems and Organizations”

NIST SP 800-171 r2 “Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations”

NIST SP 800-171a “Assessing Security Requirements for Controlled Unclassified Information”

NIST SP 800-172 “Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171”

Certifications & Assessments

The Federal Risk and Authorization Program (FedRAMP)

Established in 2011 to provide a cost-effective, risk-based approach for the adoption and use of cloud services by the federal government.

Required for all commercial cloud service offerings (CSO) to be used by a federal agency.

Cybersecurity Maturity Model Certification (CMMC)

Is the unifying standard designed to protect sensitive unclassified information that is shared by the Department with its contractors and subcontractors.

Required for all members of the Defense Industrial Base.

Considerations & Penalties

The Christian Doctrine

The Christian doctrine provides that if a statute or a regulation with the "force and effect of law" mandates the inclusion of a clause in a government contract, the courts and boards will interpret the contract as if it contains the omitted clause.

False Claims Act

The False Claims Act sets penalties at $5,000 to $10,000 per violation. However, subsequent federal law periodically adjusts the amounts for inflation. As of June, 2020, FCA penalties range from $11,665 to $23,607 per violation.

The CISO Handbook

The CISO Handbook was created to educate and inform new and existing CISOs about their role in Federal cybersecurity. It provides resources to help CISOs responsibly apply risk management principles to help Federal agencies meet mission objectives, and makes CISOs aware of laws, policies, tools, and initiatives that can assist them as they develop or improve cybersecurity programs for their organizations.

CMMC Resources & Links

CMMC Model Overview

This document focuses on the CMMC model. The model encompasses the basic safeguarding requirements for FCI specified in Federal Acquisition Regulation (FAR) Clause 52.204-21 and the security requirements for CUI specified in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 Revision (Rev) 2 per Defense Federal Acquisition Regulation Supplement (DFARS) Clause 252.204-7012 [3, 4, 5]. DFARS clause 252.204-7012

CMMC Resources & Links (cont.)

CMMC Level 1 Self Assessment Guide

This document provides self-assessment guidance for Level 1 of the Cybersecurity Maturity Model Certification (CMMC).

CMMC Level 2 Assessment Guide

This document provides assessment guidance for conducting Cybersecurity Maturity Model Certification (CMMC) assessments for Level 2.

CMMC Level 1 Scoping Guidance

Provides guidances for OSC's for determination of which assets within the contractor's environment will be assessed and the details of the self-assessment.

CMMC Level 2 Scoping Guidance

This document provides information on the categorization of assets that, in turn, inform the specification of assessment scope for a Cybersecurity Maturity Model Certification (CMMC) assessment.

For more information on Cybersecurity and Federal Government solutions go to www.schellman.com

CLICK FOR MORE INFO

www.schellman.com

4010 W Boy Scout Blvd, Suite 600 / Tampa, FL 33607 / 1.866.254.0000
Outside of the United States, please dial: +1.813.288.8833