HOW GOVERNMENT DOES CYBERSECURITY

In the face of mounting threats, government has established cybersecurity as a top priority. But how exactly will local, state, and federal agencies accomplish the mission of securing critical information and infrastructure? Rather than taking on threats alone, every facet of government has to work together to create a comprehensive and robust cyber strategy. Each employee, department, branch, and level of government has a role to play.

SPONSORED BY:

CISCO ForeScout immixGroup Cyber Security Technologies intel Security NetApp THUNDERCAT TECHNOLOGY

PRODUCED BY:

govloop

SOURCES:

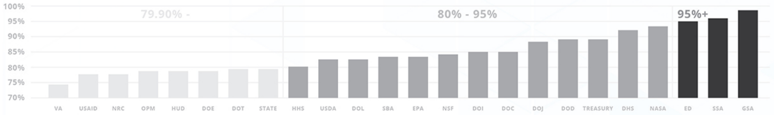
Congressional Research Service (CRS)
Performance.gov
Government Accountability Office (GAO)

THE LEADERSHIP

Chief Information Officer	Coordinate network configuration and management with security personnel to create an integrated, secure IT system
Chief Security Officer	Ensure that physical security systems are integrated with information security procedures and technologies
Chief Information Security Officer	Plan, deploy, and continuously monitor information security technologies and procedures to ensure efficacy and regulatory compliance
Chief Administrator	Provide strategic direction for agency cybersecurity policies
Agency Secretary	Liaise with other agencies and executive branch to guarantee agency policies are integrated with government-wide policies and best practices
CXO (Anyone Else)	Educate all employees about basic cyber hygiene, insider threat mitigation, and phishing scam detection

THE AGENCIES

AVERAGE CAP GOAL COMPLETION BY AGENCY - FY 2014 Q4



THE LEGISLATION

Federal Information Security Management Act (FISMA)

2014

- Requires each agency to "develop, document, and implement" information security risk management standards
- Encourages agencies to use automated security tools to continuously diagnose and mitigate security vulnerabilities
- Annually audits and rates agencies based on FISMA standards

National Cybersecurity Protection Act

2014

- Officially authorized DHS's National Cybersecurity and Communications Integration Center to act as a critical interface for sharing cybersecurity information among federal civilian agencies and key stakeholders
- Strengthens DHS's ability to coordinate incident response and provide technical assistance to agencies

Cybersecurity Enhancement Act

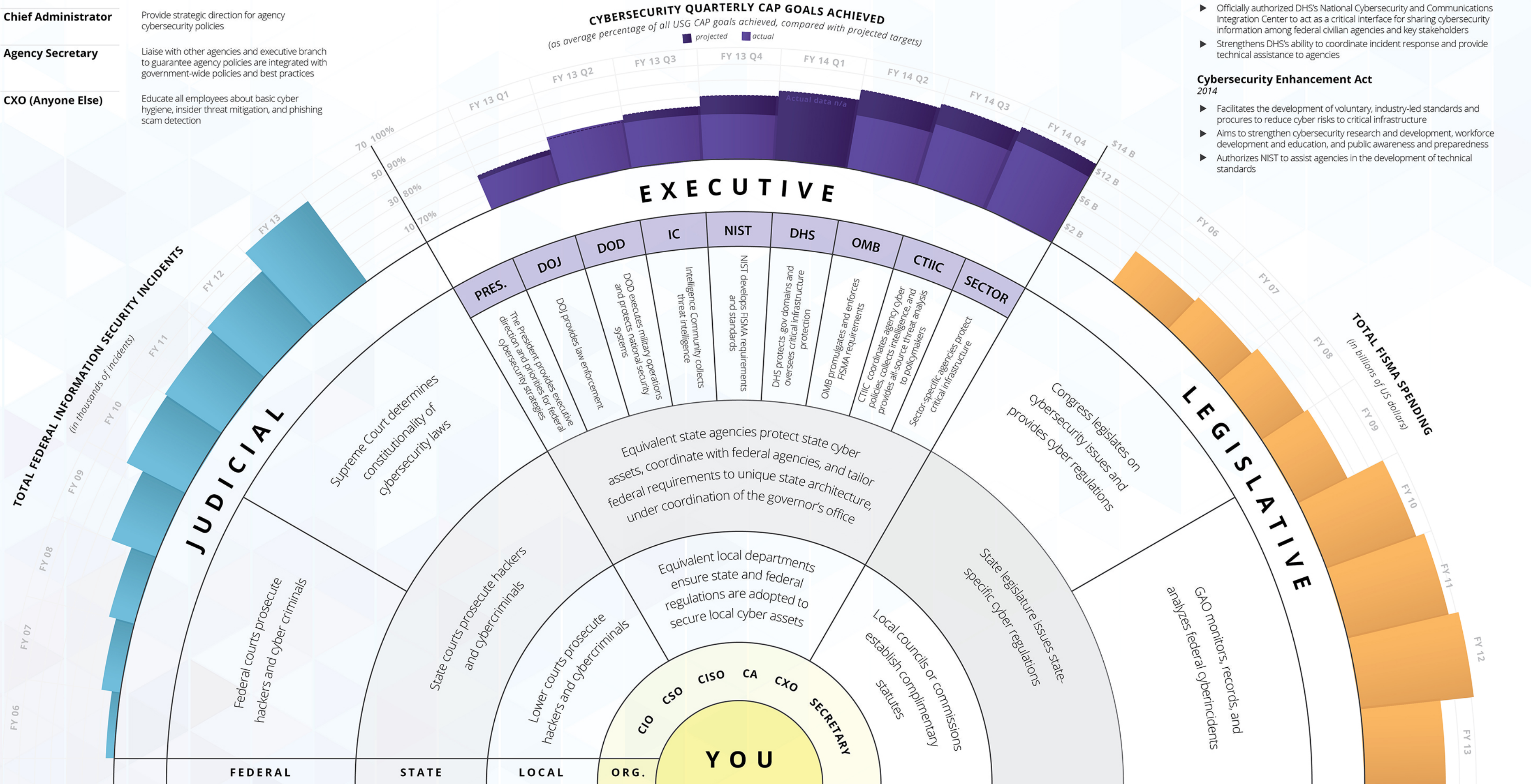
2014

- Facilitates the development of voluntary, industry-led standards and procures to reduce cyber risks to critical infrastructure
- Aims to strengthen cybersecurity research and development, workforce development and education, and public awareness and preparedness
- Authorizes NIST to assist agencies in the development of technical standards

CYBERSECURITY QUARTERLY CAP GOALS ACHIEVED
(as average percentage of all USG CAP goals achieved, compared with projected targets)

TOTAL FEDERAL INFORMATION SECURITY INCIDENTS
(in thousands of incidents)

TOTAL FISMA SPENDING
(in billions of US dollars)



EXECUTIVE

PRES. The President provides executive direction and priorities for federal cybersecurity strategies

DOJ DOJ provides law enforcement

DOD DOD executes military operations and protects national security systems

IC Intelligence Community collects threat intelligence

NIST NIST develops FISMA requirements and standards

DHS DHS protects .gov domains and oversees critical infrastructure protection

OMB OMB promulgates and enforces FISMA requirements

CTIIC CTIIC coordinates agency cyber policies, collects intelligence, and provides all-source threat analysis to policymakers

SECTOR Sector-specific agencies protect critical infrastructure

Equivalent state agencies protect state cyber assets, coordinate with federal agencies, and tailor federal requirements to unique state architecture, under coordination of the governor's office

Equivalent local departments ensure state and federal regulations are adopted to secure local cyber assets

JUDICIAL

Supreme Court determines constitutionality of cybersecurity laws

Federal courts prosecute hackers and cyber criminals

State courts prosecute hackers and cybercriminals

Lower courts prosecute hackers and cybercriminals

LEGISLATIVE

Congress legislates on cybersecurity issues and provides cyber regulations

GAO monitors, records, and analyzes federal cyberincidents

State legislature issues state-specific cyber regulations

Local councils or commissions establish complimentary statutes

CIO CSO CISO CA CXO SECRETARY

YOU

FEDERAL STATE LOCAL ORG.