FY 2018 BUDGET BLUEPRINT

- President’s Management Agenda
  - Identifies cybersecurity as a critical area to improving the federal government

- Department of Homeland Security
  - $1.5B to protect Federal networks and Critical Infrastructure from cyber attacks

- Department of the Treasury
  - $12.1B total discretionary spending, a $519M decrease from the 2017 CR level
    - enhance existing security systems
    - consolidate information technology management across the bureaus
    - Strengthens NASA’s cybersecurity capabilities, safeguarding critical systems and data
FY 2018 BUDGET BLUEPRINT CONT.

• Department of Defense
  • $52B increase from FY 2017 CR level
    • Build cyber capabilities in armed forces
    • Supports grid resiliency through Office of Electricity Delivery and Energy Reliability (OEDER)

• Department of Justice
  • $27.7B with a $1.1B decrease from 2017 CR
  • FBI to see a $249M increase from 2017 CR dedicated to
    • $61 counter terrorism, combat foreign intelligence and cyber threats “and national security risks that result from malicious actors’ use of encrypted products and services”
• Executive Order on Cybersecurity?
  
  • Jan. 28th draft E.O. on Cybersecurity

• Consistent with National Commission on Enhancing National Cybersecurity 100 page report issued in December 2016

• Agency heads plan for deliberate modernization of the federal executive branch IT

• Oversight Hearing on Cyber agency implementation March 28th, 2017
  
  • Agency progress and next steps
  • Primary issues of focus
FEDERAL LEGISLATION OUTLOOK

• Appropriations through 2017
  • CR for FY 17
  • Full budget with possible blueprint changes for FY 2018

• The 115th congress has introduced 36 bills on cybersecurity
  • No bills reached a floor vote
  • State focused legislation is on providing resources and leveraging current capabilities across federal/state/local networks
FEDERAL LEGISLATION TRENDS

• Bi-Partisan and Bicameral

• Leveraging Existing Resources
  • NCCIC, Fusion Centers, NIST and other federal resources to collect, disseminate and enhance cyber capabilities across state, local and private sector (H.R. 584; S.412; H.R. 1224; S.770)

• Workforce
  • Codify DHS mission to attract and retain highly trained computer and information security professionals (H.R.935; H.R. 1981)
  • Department of Defense Cyber Scholarship Program Act of 2017 (H.R. 1609; S.754)
FEDERAL LEGISLATION TRENDS CONT.

• Federal Consortiums, Committees and Centers
  • Study to create a Civilian Cyber Defense National Resource housed in DHS (H.R. 54)
  • Establishing a Select Committee on Cybersecurity (S.Res. 23)

• Federal Consortiums, Committees and Centers
  • FCC establish an interagency communications security committee (H.R. 1340)
  • Preparedness consortium to support efforts to address cybersecurity risks and incidents (H.R. 1465; S. 594)
FEDERAL LEGISLATION TRENDS CONT.

• IT Modernization
  
  • DHS to provide Research, development projects (H.R. 239; S.278)
  
  • Ensure federal website functionality and security for sites that collect PII (H.R. 404)

• Infrastructure
  
  • Airlines – S.679
  
  • Energy grid (S.79); critical infrastructure (H.R. 940); communication systems (H.R. 1335)
  
  • Cars: NHTSA recommend standards for regulation of cybersecurity of motor vehicles (S.680; H.R. 701)
  
  • Elections/Voter Machines H.R. 1907
STATE RESOURCES

S. 412 - "State and Local Cyber Protection Act of 2017"

• Require the NCCIC to assist state and local governments with cybersecurity

H.R. 1344 "State Cyber Resiliency Act". Companion Bill S. 516

• Establishes a State Cyber Resiliency Grant Program

  • Up to 2 planning grants to develop or revise a cyber resiliency plan; or

  • Up to 2 implementation grants to implement an active cyber resiliency plan
CYBERSECURITY FEDERAL UPDATE

Washington, D.C. Office
• Susan Frederick, susan.Frederick@ncsl.org
• Danielle Dean, Danielle.dean@ncsl.org

Denver, CO Office
• Pam Greenberg, Pam.Greenberg@ncsl.org
• Heather Morton, Heather.Morton@ncsl.org