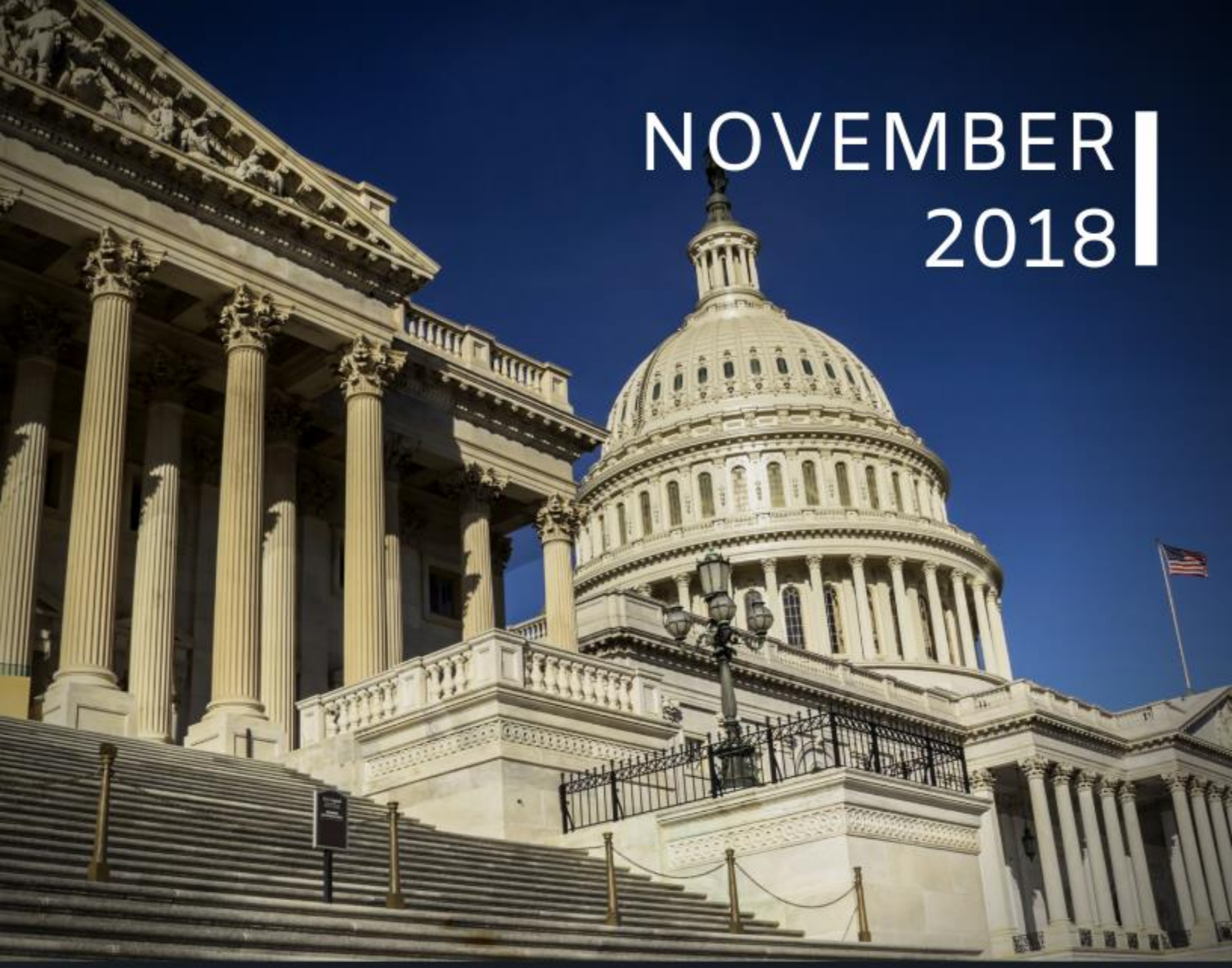

NOVEMBER 2018

THE ICIT FEDERAL CYBERSECURITY INITIATIVE REPORT

A MONTHLY UPDATE FROM THE INSTITUTE FOR CRITICAL INFRASTRUCTURE TECHNOLOGY

ICIT | Institute for Critical Infrastructure Technology

The Cybersecurity Think Tank

The ICIT Cyber Federal Cybersecurity Initiative Report

November 2018

A Monthly Non-Partisan Report from The Institute for Critical Infrastructure Technology

www.icitech.org

Contents

About this Report

As a non-partisan cybersecurity think tank, one of ICIT's goals is to increase access and visibility on federal agency cybersecurity and privacy related initiatives or agency decisions. This monthly members-only report is an objective summary of various federal agency programs, announcements, reports, and other initiatives deemed significant by ICIT analysts.

Readers should note the following:

- Highlighted items new initiatives added since the previous months report
- ICIT will keep legislation on the report for 3 months
- This report primarily tracks initiatives that ICIT analysts define as 'cyber-centric', meaning its primary focus is cybersecurity, information security or digital privacy

Department of Defense (DOD)

GAO Report Finds U.S. Weapons Systems Vulnerable to Cyber Attack

Introduced - November 2018

Summary: A 50-page GAO report issued to the U.S. Senate Armed Services Committee found that U.S. weapons systems are, almost across the board, highly vulnerable to cyber-attack. The report asserts that the Department of Defense (DoD) has gotten off to "a late start" in prioritizing cybersecurity, and has only "a nascent understanding" of how to develop more protected weapons systems.

Reference Link

- GAO targets DoD cyber vulnerability

Recalled Changes to Contractor Pay Schedule

Introduced - November 2018

Summary: In August 2018, the Pentagon unveiled a plan to pay contractors based on the performance of their contracts. In response to industry pushback, the Department of Defense rescinded their support for the plan in November.

Reference Link

- DoD recalls controversial contractor pay schedule change

Initiated the Separation of CYBERCOM from NSA

Introduced - November 2018

Summary: The separation of CYBERCOM from NSA was an idea initiated during the Obama administration and was included in defense authorization legislation for fiscal 2017. The Air Force has awarded Northrop Grumman a $54 million labor-hour and cost contract to build out the "Unified Platform" for military cyber operations, a capability critical to eventually separating U.S. Cyber Command from the National Security Agency.

Reference Links

- DOD takes initial steps in separating CYBERCOM from NSA

Deliver Uncompromised

Introduced - October 2018

Summary: The Pentagon is considering implementing MITRE's framework designed to instill security into the acquisition process.

Reference Links

- Pentagon pursues more secure IT purchasing via Deliver Uncompromised initiative

Department of Energy (DOE)

OIG Report Highlights Recurring Issues in DOE Systems

Introduced - November 2018

Summary: The Department of Energy (DoE) Office of Inspector General (OIG) released a report that found several weaknesses in the cybersecurity program at DoE in fiscal year 2018, including recurring issues in vulnerability management, patching, and formal cybersecurity training policies.

Reference Links

- OIG Flags Persistent Cyber Weaknesses at New DoE Locations

Awarded $46M to Mitigate Cyber-Physical Threats to Solar Grid

Introduced - November 2018

Summary

The U.S. Department of Energy (DOE) will award $46 million in research funding to 10 projects over the next three years with amounts varying from $2 to $10 million in size, to advance strategies to mitigate cyber and physical threats to solar energy grids. Applicants are encouraged to work with local municipalities – including state, local, tribal, and territories — to take steps to manage cyber and physical threats to improve the resiliency of solar-generated electricity.

Reference Links

- DOE to award $46M to mitigate cyber, other threats to solar grid

---

Pipeline Cybersecurity Initiative

Introduced - October 2018

Summary

The Pipeline Cybersecurity Initiative will leverage the unique expertise of DoE, DHS, TSA, and other Federal agencies to support the efforts of the Oil and Natural Gas Subsector Coordinating Council to address the threats to the nation's pipelines.

For More Information on Receiving the Monthly ICIT Federal Cybersecurity Initiative Report Please Visit
https://icitech.org/federal-initiatives/

or contact ICIT at info@icitech.org