US govt grants academics $12M to develop cyberattack defense tools

By **Sergiu Gatlan (https://www.bleepingcomputer.com/author/sergiu-gatlan/)** April 22, 2022 12:33 PM 0

The US Department of Energy (DOE) has announced that it will provide $12 million in funding to six university teams to develop defense and mitigation tools to protect US energy delivery systems from cyberattacks.

Cybersecurity tools developed as a result of the six university-led research, development, and demonstration (RD&D) projects will focus on detecting, blocking, and mitigating attempts to compromise critical controls within the US power grid.

The teams behind these RD&D projects funded by the US government will also work on innovative technology that will enable energy delivery systems to survive and recover quickly following cyberattacks.

"DOE's Office of Cybersecurity, Energy Security, and Emergency Response (CESER) will fund six university teams to perform cybersecurity RD&D to advance anomaly detection, artificial intelligence and machine learning, and physics-based analytics to strengthen the security of next-generation energy systems," DOE said.

"These systems include components placed in substations to detect cyber intrusions more quickly and automatically block access to control functions."

The complete list of university teams and projects funded by DOE CESER includes:

- **Florida International University:** artificial intelligence (AI)-based detection tools and design effective cyber threat mitigation strategies using these technologies.
- **Iowa State University:** defense-in-depth security and resilience for cyber-physical systems using AI-integrated, attack-resilient, and proactive system technologies and solutions.
- **New York University:** a program called Tracking Real-time Anomalies in Power Systems (TRAPS) to detect and localize anomalies in power grid cyber-physical systems.
- **Texas A&M Engineering Experiment Station:** will leverage AI and machine learning to develop techniques and scalable prototypes for intrusion response against advanced cyber-physical threats to power systems.
- **University of Illinois at Chicago:** a resilient, next-generation solid-state power substation, integrating cybersecurity considerations to improve adoptability.
- **Virginia Polytechnic Institute and State University:** a program called Cyber REsilience of SubsTations (CREST), a two-part system to detect and mitigate cyber incidents while maintaining secure communication and critical functions.

(https://twitter.com/DOE_CESER/status/1517193107338637314)

DOE's announcement comes after two joint advisories from the US government in January (https://www.bleepingcomputer.com/news/security/us-govt-warns-of-

russian-hackers-targeting-critical-infrastructure/) and from Five Eyes nations on Wednesday (https://www.bleepingcomputer.com/news/security/us-and-allies-warn-of-russian-hacking-threat-to-critical-infrastructure/), warning of an increased risk that Russian-backed hacking groups could target critical infrastructure organizations worldwide.

The FBI also revealed in its Internet Crime Complaint Center (IC3) 2021 Internet Crime Report that ransomware gangs breached at least 649 organizations (https://www.bleepingcomputer.com/news/security/fbi-ransomware-hit-649-critical-infrastructure-orgs-in-2021/) from multiple US critical infrastructure sectors last year.

Since the start of the year, the FBI has issued other alerts highlighting how ransomware gangs, including BlackByte (https://www.bleepingcomputer.com/news/security/fbi-blackbyte-ransomware-breached-us-critical-infrastructure/), Ragnar Locker (https://www.bleepingcomputer.com/news/security/fbi-ransomware-gang-breached-52-us-critical-infrastructure-orgs/), and Avoslocker (https://www.bleepingcomputer.com/news/security/fbi-avoslocker-ransomware-targets-us-critical-infrastructure/), targeted and hacked dozens of critical infrastructure organizations across the United States.

Earlier in April, a joint cybersecurity advisory from CISA, NSA, FBI, and the Department of Energy (DOE) also warned of government-sponsored hacking groups using a new ICS-focused malware toolkit (tracked as PIPEDREAM or INCONTROLLER) (https://www.bleepingcomputer.com/news/security/us-warns-of-govt-hackers-targeting-industrial-control-systems/) to hijack industrial control system (ICS) and supervisory control and data acquisition (SCADA) devices.

The FBI, CISA, and the NSA advised US critical infrastructure orgs (https://www.bleepingcomputer.com/news/security/us-govt-warns-of-russian-hackers-targeting-critical-infrastructure/) to focus on detecting their malicious activity by enforcing robust log collection/retention and monitoring them for behavioral evidence or network and host-based artifacts.