MINUTES

HOUSE ENVIRONMENT, ENERGY & TECHNOLOGY COMMITTEE

DATE:	Tuesday, February 28, 2017
TIME:	1:30 P.M.
PLACE:	Room EW41
MEMBERS:	Chairman Raybould, Vice Chairman Thompson, Representatives Hartgen, Vander Woude, Anderson, Anderst, Mendive, Trujillo, Chaney, Nate, Cheatham, Horman, Malek, Moon, Smith, Scott, Jordan, Rubel
ABSENT/ EXCUSED:	Rep. Vander Woude, Rep. Anderson, Rep. Chaney, Rep. Scott, Rep. Malek, Rep. Moon
GUESTS:	John Chatburn, Governor's Office of Energy and Mineral Resources

Chairman Raybould called the meeting to order at 1:31 p.m.

MOTION: **Rep. Jordan** made a motion to approve the minutes of February 20, 2017. **Motion carried by voice vote.**

Zach Tudor, Associate Laboratory Director, National Department Homeland Security (DHS), Idaho National Laboratory (INL). Mr. Tudor also serves as a member of the Board of Directors of the International Information System Security Certification Consortium (ISC), that provides strategy, governance and oversight for the Certified Information Systems Security Profession (CISSP) certification that grants certifications to qualifying candidates and enforces adherence to the ISC Code of Ethics. INL experts conduct control system cybersecurity research, travel across the nation to large industrial sites, communities and military facilities to participate in cyber security investigations and security assessments of critical infrastructure, collaborate with government agencies, private industries, universities and via ICS-CERT staff respond to calls from government and industry representatives requesting help regarding suspect cyber-related events, and, at the invitation of the Department of Energy (DOE) and the International Atomic Energy Agency, share expertise to improve cybersecurity at nuclear power plants and other critical infrastructure in foreign countries. They are also assisting nuclear energy plants and other utilities across the nation to implement more secure systems and leading in the development and implementation of Consequence-driven Cyber-informed Engineering addressing cyber attack. Since cyber attacks can happen to automobile control systems, INL has developed cooperative research agreements with auto manufacturers to assist them in producing cybersecure vehicles.

Under a consolidated Battelle Energy Alliance contract in 2005, the DOE and INL invested approximately $100 million to enable cybersecurity research and develop laboratories and a power-grid test bed. INL, DOE, DHS and the Department of Defense develop, test and validate technologies, systems and policies to protect the nation's critical infrastructures via the Critical Infrastructure Test Range Complex (CITRC). INL has designated nearly $4 million for creation of the Cybercore Integration Center, has 51 contracts worth $9 million with universities in Idaho to perform collaborative research, and cosponsors the Center for Advance Energy Studies and K-12 STEM.

In response to committee questions, **Mr. Tudor** replied that he would need to research and report back to the committee on whether INL has ever been hacked, whether over-the-horizon technology is a cyber threat to INL, and whether flights over INL pose a cybersecurity risk. Mr. Tudor informed committee members in answer to a question that hacking into driverless cars is a possibility, which is why INL and DHS are working to understand the systems and to make them safer. Mr. Tudor defined CITRC, when asked by committee members, as the Critical Infrastructure Test Range Complex, which has a wireless test bed, power generation and electric distribution lines and is a platform allowing INL to bring in other tools from utilities to test in a real environment. CITRC also has water test beds, roads and rails, so they can have a complete environment to simulate a small region for testing real-world scenarios.

Dick Garlish, General Manager of Compliance Risk and Security, Idaho Power, defined Idaho Power's cybersecurity levels and gave a brief explanation for the increasing need for cybersecurity. Since 2011, Idaho Power had 10 million breach attempts to their corporate perimeter, and this year 8 people got in, but Idaho Power was able to isolate, contain and mitigate their threat. Idaho Power uses industrial control systems to run their generation and distribution network to their customers, and because it is a huge concern, Idaho Power has invested more than $13 million since 2012 in cybersecurity protections, including 8 full-time employees dedicated to watching their network and environment and mitigating problems. Idaho Power spends 7 1/2% of a $34 million internet technology budget on cybersecurity. Mr. Garlish discussed the types of data both Idaho Power's corporate and operation environment levels have and how they are protected. He explained that at the operational environment level, they use a lot of automatic systems to ramp up and ramp down, and INL helps put in a lot of protection schemes, which is a tremendous asset. Idaho Power participates in INL training and conducted an evaluation this year. Threats change all the time, and Idaho Power is happy to have the support of INL.

In response to committee questions, **Mr. Garlish**, explained that Idaho Power participates in EEI, a national trade organization for utilities and the successor to the US CERT, a government facilitated information sharing site, to help improve their security posture.

ADJOURN: There being no further business to come before the committee, the meeting adjourned at 2:10 p.m.

_____
Representative Raybould
Chair

_____
Lorrie Byerly
Secretary