Sandia National Laboratories

Energy, Climate & Infrastructure Security

The Infrastructure Security program area works to develop and apply technologies/analytical approaches to secure the nation's critical infrastructure against natural or malicious disruption.

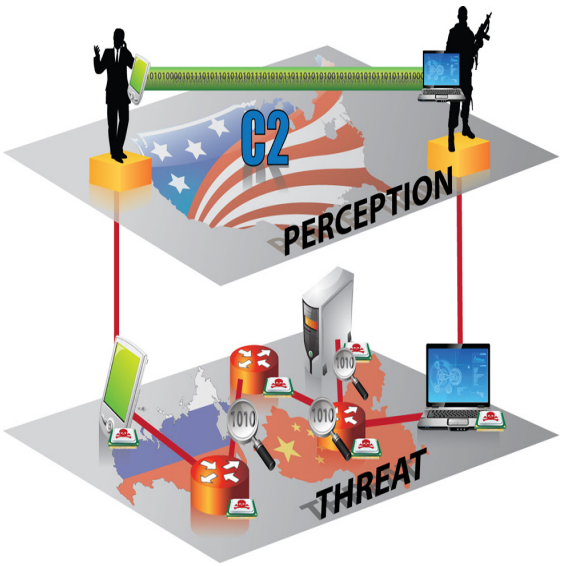
Vision

To enhance the nation's security and prosperity through sustainable, transformative approaches to our most challenging energy, climate, and infrastructure problems.

Goal: Establish and grow critical cybersecurity capabilities within the Department of Homeland Security with Sandia as the enduring advanced development partner.

The Department of Homeland Security (DHS) has the mission of protecting civilian federal government information networks against a full range of threats. Government networks and servers are repositories of vast amounts of information that, if stolen, could compromise Americans' physical safety and security as well as their privacy and financial security. As the U.S. benefits from the past few decades' technological advances, we increase our dependence on interconnected devices and systems. This dependence creates vulnerabilities, which might be exploited by adversaries ranging from criminal organizations through nation states. The complexity of these interconnected systems and the rate of technological change cries out for a national-lab-level approach to mitigate the risks to our government systems and our critical computer infrastructures.

Sandia's goal is to develop game-changing cybersecurity capabilities to support DHS's mission of securing the nation's ".gov" domain and defending critical civil, industrial, and commercial infrastructures from cyber-based vulnerabilities. We will evaluate systems with the potential to impact critical



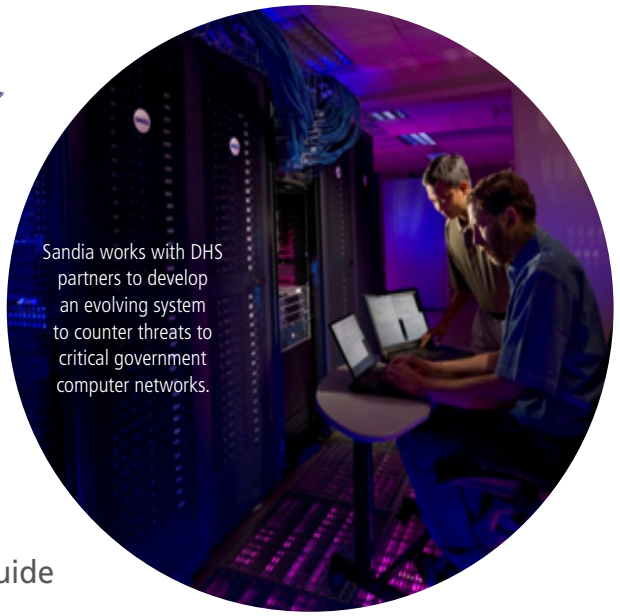
Effective cybersecurity is transparent to the legitimate network user, but secure against emergent threats from malicious agents.

U.S. DEPARTMENT OF ENERGY

Software products come to us from all over the world. We must be vigilant that malicious code is never allowed to institute itself into our critical civil and military computer systems and networks.

infrastructures for supply-chain vulnerabilities and create mitigation strategies for supply-chain-induced risks. We will devise strategies to extend cybersecurity beyond government assets to the telecommunications providers, industry partners and subcontractors, and to global partners. Lastly, we will develop a scalable process to assess and improve the cybersecurity performance of government agencies and critical infrastructures, with the objective of providing agencies a mechanism for sharing threat, compromise, and mitigation data.

Our goal is to build/use a threat model in order to guide development, acquisition, and operation of a protective system. The complexity and scale of this system will be unprecedented; it must scale over a wide range of attributes: network size, data sensitivity, communications capacity, geographical distribution, and operational authorities. Sandia is contributing to the solution by providing architectural designs based on threat models. We are providing much needed scalability to the efforts to address the cyber risks. We are tackling the big problems, like the supply-chain risk, which are so challenging as to be largely deferred by the other contributors to cybersecurity.



Sandia works with DHS partners to develop an evolving system to counter threats to critical government computer networks.

For more information please contact:

Robert Hutchinson
E-mail: rlhutch@sandia.gov
Phone: (925) 294-4531
Website: www.energy.sandia.gov

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND2011-1819P