

## WHY SANDIA?

Sandia's history of providing adversarial threat assessment for the U.S. Nuclear Command and Control Systems has given us an unusually rich understanding of the threats that can be employed to compromise even the most carefully protected systems. This knowledge has been integrated into Sandia's rigorous cradle-to-grave lifecycle approach for developing information security approaches, technologies and systems.

Sandia's cyber security R&D program draws heavily upon our core S&T capabilities developed over decades in support of national security. These S&T investments afford the nation the ability to leverage world-leading capabilities in advanced informatics, microelectronics, and modeling and simulation. Sandia's differentiating value, among other R&D institutions, comes from our unique systems approach that integrates scientific understanding, technology development, and complex requirements-driven engineering to develop solutions that work effectively within the broader context of their intended deployment environment and operational mission.

Sandia works effectively as an innovation hub to build and lead collaborations with academia, industry, and government partners, by leveraging its deep science and technology base and rich security system engineering, design, and integration tradition. We foster innovation through our unique ability for recursive and non-linear integration of science and understanding, missions and users, and tools and technology. Sandia invests in solving the nation's most challenging cyber problems, assuming technical risks that others cannot or will not accept.

## For More Information:

Please visit:  
[www.sandia.gov/cyber](http://www.sandia.gov/cyber)

[www.sandia.gov/bus-ops/partnerships](http://www.sandia.gov/bus-ops/partnerships)



## RESEARCH & DEVELOPMENT SOLUTIONS

Sandia has long-standing relationships with key government agencies that have allowed us to develop a comprehensive understanding of mission needs and constraints. Our cyber analysis, assessment, reverse engineering, design and development capabilities are distinguished by a broad science and technology base with differentiating capabilities in trusted systems engineering and scalable informatics.

## COLLABORATION/PARTNERSHIPS

Sandia supports a variety of organizations, committees, panels, advisory boards and strategic studies in our effort to secure our nation's cyber space. Our customers are responsible for a broad spectrum of infrastructure critical to maintaining national security, ranging from vital military capabilities to the private industries that support our societal needs.

### Our sponsors and partners include:

- Department of Energy (DOE)
- Department of Defense (DOD)
- Department of Homeland Security (DHS)
- The intelligence community
- Members of the banking industry
- Power companies
- Software development companies
- Other research laboratories



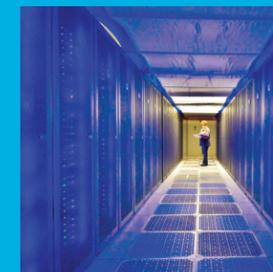
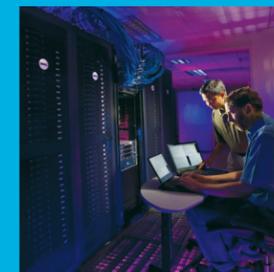
## SANDIA'S CYBER SECURITY RESEARCH PROGRAM

Enabling technologies and solutions

Sandia provides technical leadership in threat-informed cyber security solutions required for the nation's most critical systems.

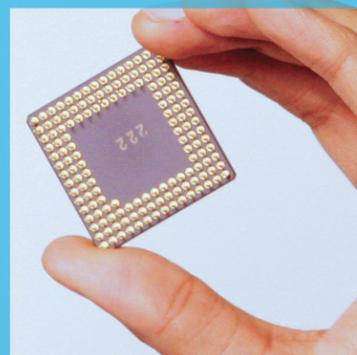


Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND 2010-5569 P



We deliver solutions that leverage our deep science and technology base and utilize a threat-informed approach to identify and mitigate cyber risks in critical national security systems.

Sandia's Center for Integrated Nanotechnologies (CINT) is helping enable quantum device measurement and characterization, and driving cutting edge GaAs quantum well research with collaborators such as Lawrence Berkeley National Laboratory and UC Santa Barbara.



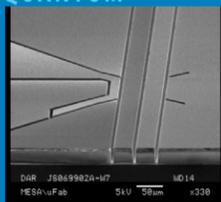
Designed and fabricated in Sandia's DoD accredited facilities, Sandia provides Trusted Components for national security applications.

**Sandia National Laboratories** is playing a fundamental role in assisting the nation both as a provider of robust security solutions and as a technical advisor on national cyber strategies. Sandia's work for the intelligence and defense communities has established a reputation of comprehensive expertise and capabilities in computer science research and development.

## SANDIA RESEARCH CONTRIBUTION

Sandia is making a broad impact on cyber security through basic and applied research activities.

### QUANTUM



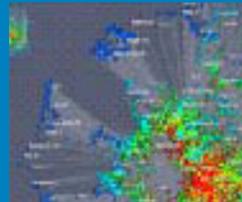
Sandia's comprehensive Quantum R&D program includes research in Si DQD, topological QC, modeling, and theory.

Sandia has a growing infrastructure supporting quantum research, with facilities and staff to support a full spectrum of research needs (solid state physics, experimental work, fabrication, simulation and systems engineering) both internal to Sandia and externally.

### EMULYTICS

Emulytics leverages Sandia's expertise in large-scale simulation and high-performance scalable computing to create emulations and simulations of cyber attacks such as malware propagation or botnets at the scale of the Internet. Sandia is currently developing the ability to run emulations on the scale of  $10^7$  distinct OS platforms and is creating the diagnostics and theory to mature this capability into a tool for cyber prediction and defense.

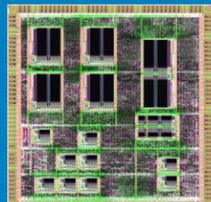
### INFORMATICS



Sandia is bringing together its research and operational expertise in computing, massive data

warehousing, software engineering, and threat analysis to develop specialized informatics-based analytical capabilities that are scalable to meet the most challenging situational awareness needs. Pioneering research includes work in scalable informatics analytics using graph theoretic approaches and novel computer architectures -- drawing upon technologies from industry partners such as Cray's multi-threaded architectures, data machines like Neteeza, and IBM's Cell processor -- to provide new insights from terascale data. Sandia's work in informatics also includes implementation of data and text mining tools, natural language processing tools, and visualization tools.

### TRUSTED SYSTEMS



In order to gain confidence that a cyber system performs in a secure and trusted manner, it must be analyzed, tested, and

independently validated to ensure that it correctly provides the desired capabilities and that it prevents adversaries from exploiting those capabilities to achieve some malicious goal. The complexity of commercially available computing resources does not lend itself to the validation of trusted and secure execution, yet we necessarily rely on these platforms for mission-critical information. Sandia develops and manufactures specialized microcircuits and microprocessors designed with security in mind to provide a reusable platform that addresses these significant issues in trusted computing.

## KEY CAPABILITIES

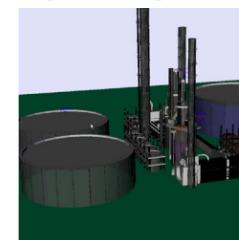
Our capabilities and expertise include:

- Development and analysis of trusted hardware and software to assure the integrity of our cyber infrastructure
- Simulation and prototyping of integrated protective systems that incorporate an understanding of the full threat spectrum
- Conducting information operations red teaming and assessments to better understand vulnerabilities
- Providing a structured approach to vulnerability assessment of both foreign and domestic systems
- Leveraging world-class scalable computational algorithms and analysis integrated with high-performance computing capabilities

*"The fact that our supercomputing capabilities are being used for intelligence missions is also an important example of how our investment in nuclear security is providing the nation the tools to tackle broader national challenges."*

—NNSA Administrator Thomas D'Agostino

### VULNERABILITY ASSESSMENT



A sophisticated, threat-informed approach to red teaming and vulnerability assessment is a customer valued asset. Sandia's

comprehensive expertise in vulnerability assessment, stemming from decades of experience evaluating mission critical systems, enables us to deliver solutions that identify and mitigate cyber risks in vital national security systems.

### MICROELECTRONICS FABRICATION

Our microsystems and microelectronics fabrication facilities combine custom-built, trustworthy design tools with techniques for leveraging untrustworthy supply chains to create high-assurance microelectronic systems.

### QUANTUM SCIENCE PROGRAM

Sandia's Quantum Science Program is leveraging silicon fabrication and other capabilities to support collaborations at facilities including Purdue, Princeton, Yale, the University of Maryland, and the Center for Quantum Computer Technology in Australia.

### HIGH PERFORMANCE COMPUTING



Sandia has a rich history of partnering with the US supercomputer industry at the very high end, often by leading industry through advances in supercomputing technology.

Sandia has led the world in adopting the successful Massively Parallel Processor (MPP) supercomputer paradigm as demonstrated in the success of the NCube, Intel Paragon and Teraflop platforms. Most recently, Sandia partnered with Cray to develop the highly successful XT and XMT lines. Sandia is currently exploring architectural issues necessary to scale to the 1-100 PFLOPS level.

*"Cray's partnership with Sandia has been one of the most significant partnerships in the company's history. Not only did our collaboration on Red Storm result in significant scientific advancements and accomplishments in support of the Department of Energy's NNSA mission, it also spawned a very successful, proven line of Cray XT supercomputers."*

—Cray CEO Peter Ungaro