This paper describes objective technical results and analysis. Any subjective views or opinions that might be expressed in the paper do not necessarily represent the views of the U.S. Department of Energy or the United States Government.

SAND2020-8738C

SANDIA CYBER OVERVIEW

PRESENTED BY

Jen Gaudioso

- Director, Homeland Security & Defense Systems

- August 2020

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

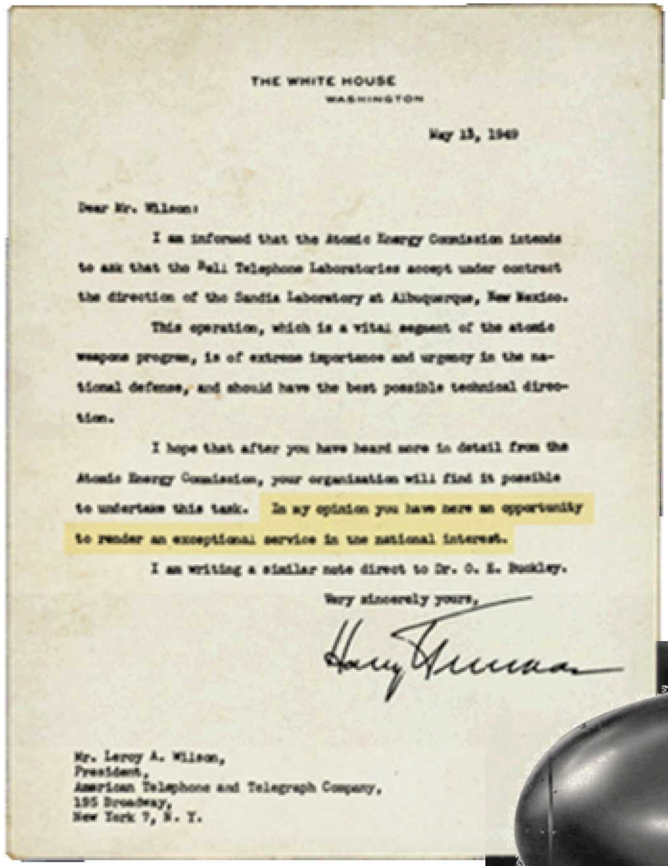
SANDIA'S HISTORY IS TRACED TO THE MANHATTAN PROJECT

…In my opinion you have here an opportunity to render an exceptional service in the national interest.

National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc.

Government owned, contractor operated

FFRDCs are long-term strategic partners to the federal government, operating in the public interest with objectivity and independence and maintaining core competencies in missions of national significance



THE WHITE HOUSE
WASHINGTON

May 13, 1949

Dear Mr. Wilson:

I am informed that the Atomic Energy Commission intends to ask that the Bell Telephone Laboratories accept under contract the direction of the Sandia Laboratory at Albuquerque, New Mexico.

This operation, which is a vital segment of the atomic weapons program, is of extreme importance and urgency in the national defense, and should have the best possible technical direction.

I hope that after you have heard more in detail from the Atomic Energy Commission, your organization will find it possible to undertake this task. In my opinion you have here an opportunity to render an exceptional service in the national interest.

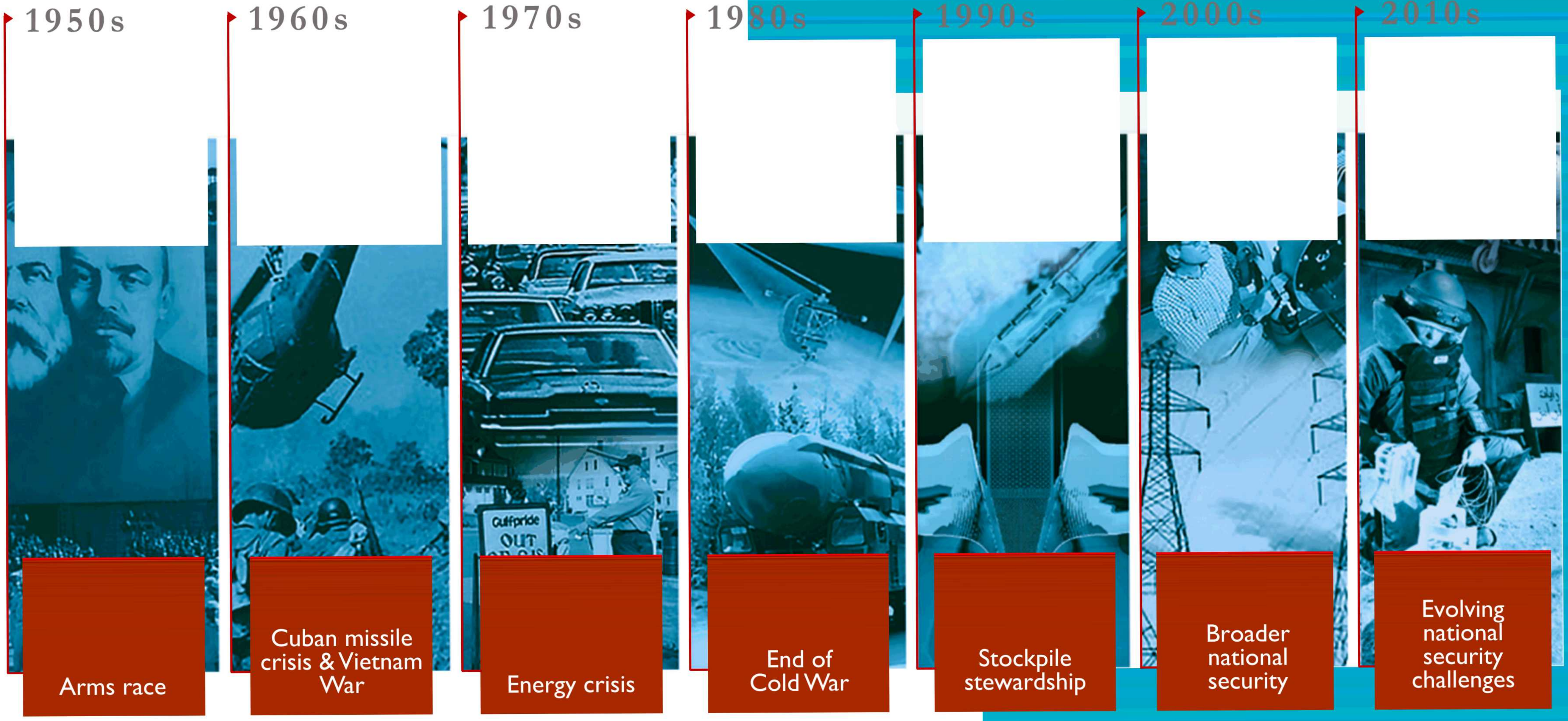
I am writing a similar note direct to Dr. O. E. Buckley.

Very sincerely yours,

Harry Truman

Mr. Leroy A. Wilson,
President,
American Telephone and Telegraph Company,
195 Broadway,
New York 7, N. Y.

SANDIA ADDRESSES NATIONAL SECURITY CHALLENGES



1950s – Arms race

1960s – Cuban missile crisis & Vietnam War

1970s – Energy crisis

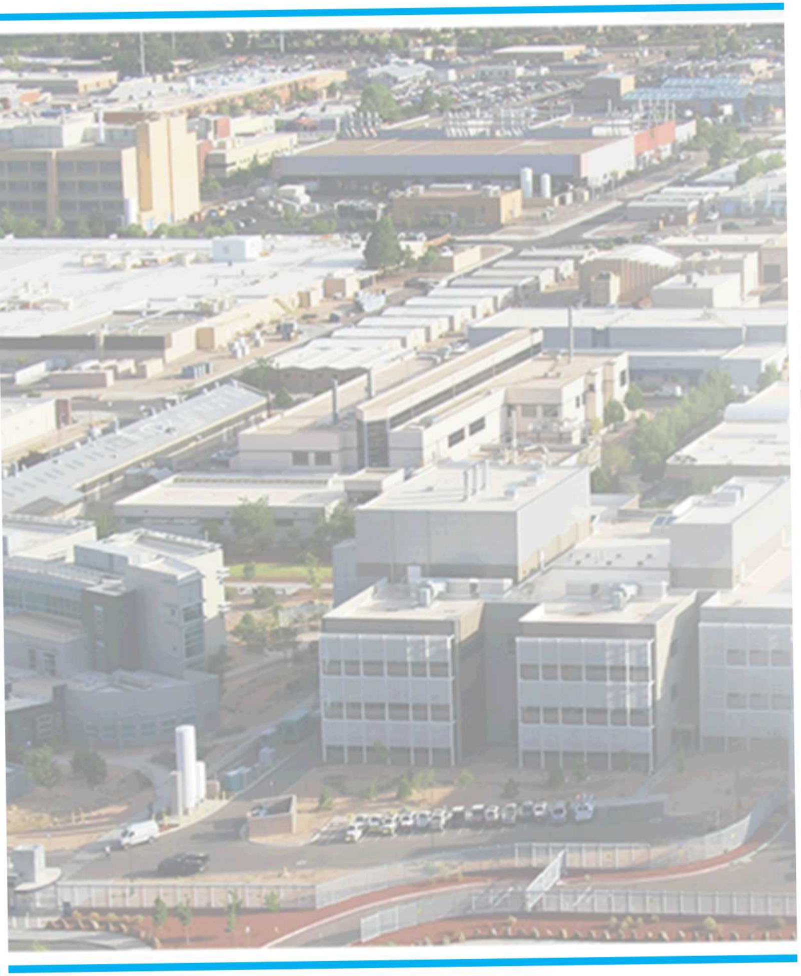
1980s – End of Cold War

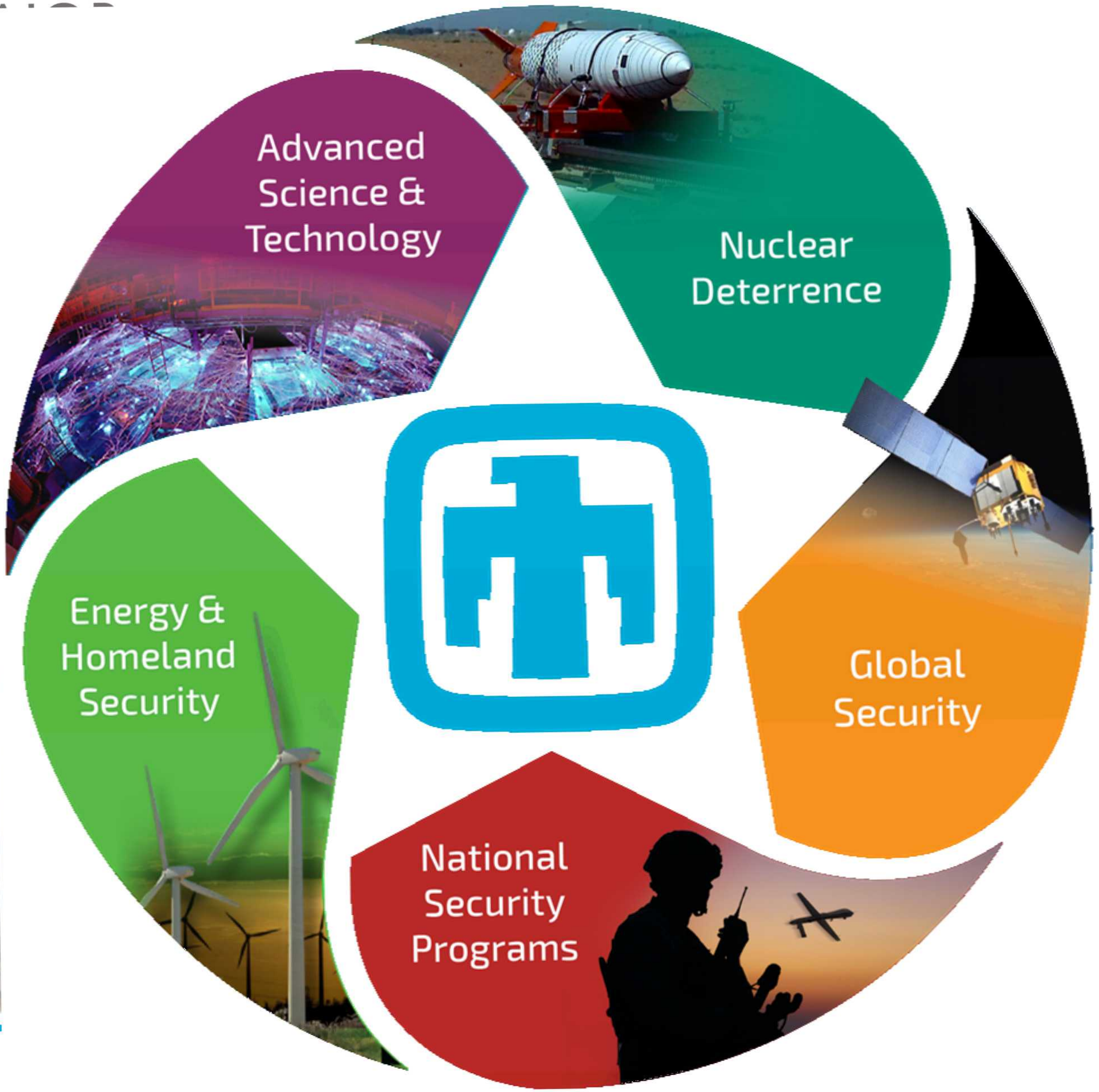
1990s – Stockpile stewardship

2000s – Broader national security

2010s – Evolving national security challenges

SANDIA HAS FIVE MA PROGRAM PORTFOL





Advanced Science & Technology

Nuclear Deterrence

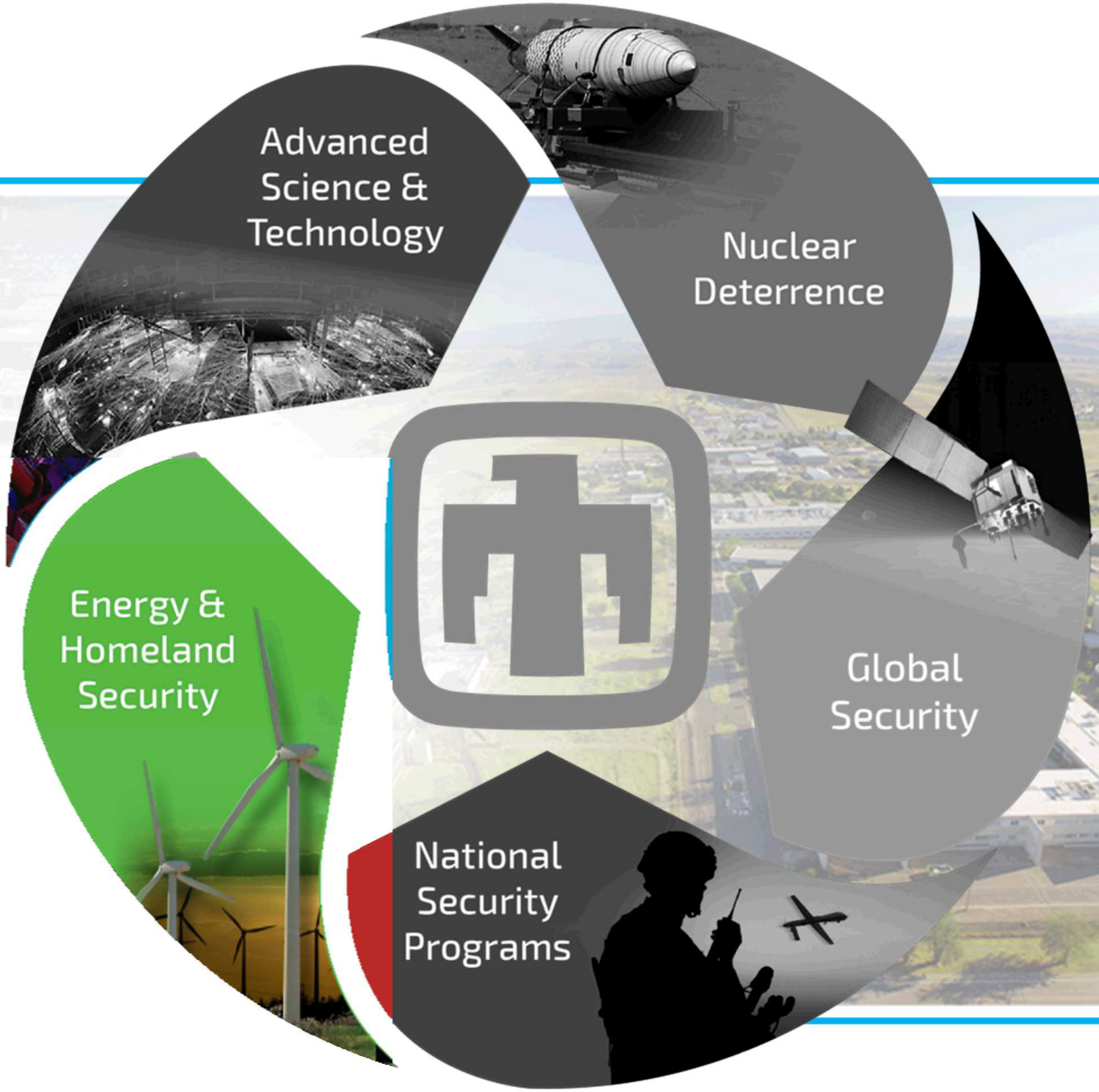
Global Security

National Security Programs

Energy & Homeland Security

SANDIA HAS FIVE MAJOR PROGRAM PORTFOLIOS

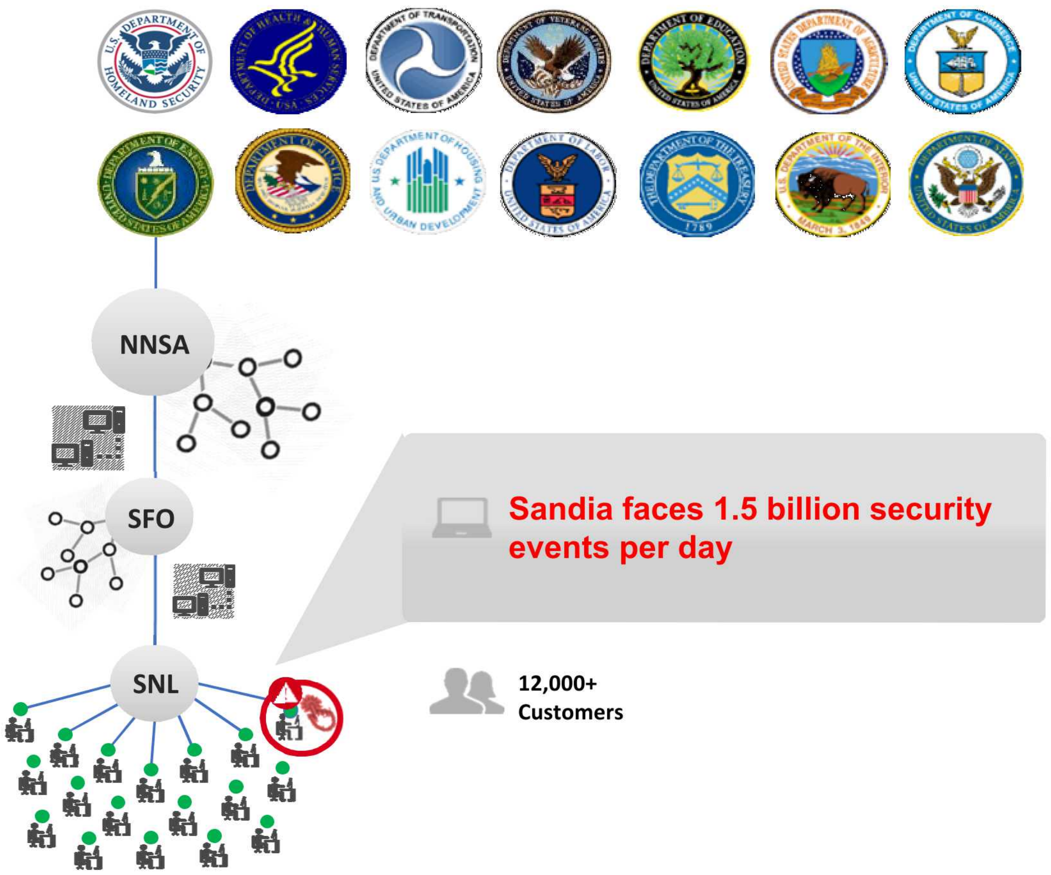
- Perform fundamental and applied R&D to support the resilience and security of the nation's energy system
- Provide protection for our nation's digital and physical critical infrastructures
- Reduce U.S. vulnerability to chemical, biological, radiological, and nuclear threats
- Accelerate transformative innovations in the transportation sector through foundational physical and computational research


Advanced Science & Technology
Nuclear Deterrence
Global Security
National Security Programs
Energy & Homeland Security

SANDIA CIVILIAN CYBER

THE CIVILIAN CYBER CHALLENGE: PROTECTING .GOV AND .COM

CIVILIAN GOVERNMENT PROTECTS 300 DEPARTMENTS & AGENCIES:



NNSA

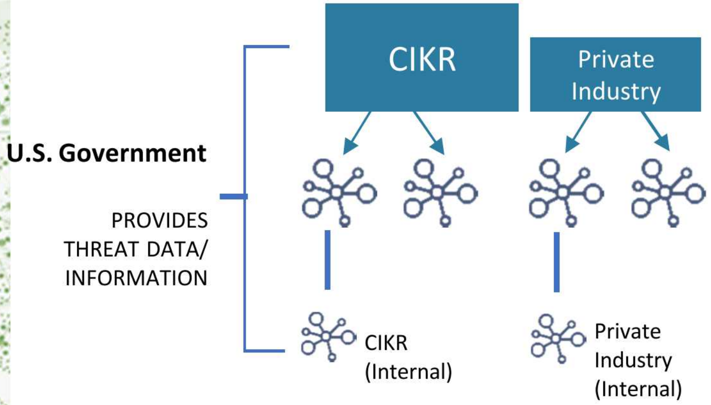
SFO

SNL

Sandia faces 1.5 billion security events per day

12,000+
Customers

CIKR/PRIVATE INDUSTRY.com (.net, .org.)



CIKR

Private Industry

U.S. Government

PROVIDES
THREAT DATA/
INFORMATION

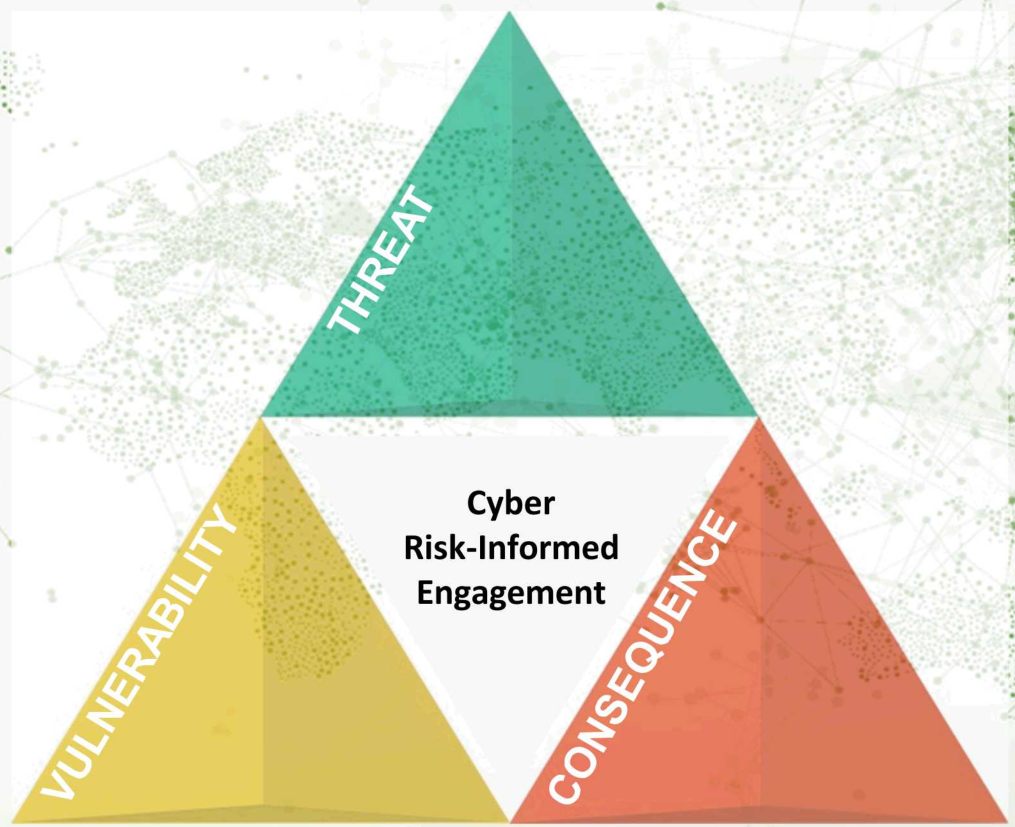
CIKR
(Internal)

Private
Industry
(Internal)

CIKR - Critical Infrastructure Key Resources

.gov is currently 2.4M people

CYBER RISK-INFORMED SUPPORT



Risk = Threat x Vulnerability x Consequence

CIVILIAN CYBER SUPPORT: CAPABILITIES OVERVIEW

Technical and engineering expertise to address unique challenges and support policy decisions in 3 key areas:

Cybersecurity Engineering

Technical expertise and development efforts seek to prevent disruption and enhance recovery capabilities by understanding changes to the technical landscape.

Cybersecurity Risk & Threat

Application of methodologies, tools, and capabilities reduces risks that affect increasingly complex and dynamic systems.

Cybersecurity Modernization

A robust understanding of the threat environment, and current engineering challenges, leads to the development of policy to drive modernization of cybersecurity services.

CIVILIAN CYBER SUPPORT: CYBERSECURITY ENGINEERING

Cybersecurity Engineering

Technical expertise and development efforts seek to prevent disruption and enhance recovery capabilities by understanding changes to the technical landscape.

OPPORTUNITIES FOR PARTNERSHIP

Malware Analysis

Enhance the capabilities of the intrusion detection services by improving the ability to discover and reverse engineer malware.

Advanced Analytics

Evolve capabilities through the addition of Threat Discovery, Behavioral Analytics, and Automated Defense.

CIVILIAN CYBER SUPPORT: CYBERSECURITY RISK & THREAT

Cybersecurity Risk & Threat

Application of methodologies, tools, and capabilities reduces risks that affect increasingly complex and dynamic systems.

OPPORTUNITIES FOR PARTNERSHIP

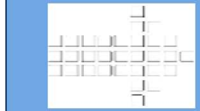
Risk Metrics

Develop algorithms to identify clusters of threat activity and threat actor capability tiers in order to communicate the value of intrusion prevention services.

Cyber Risk Methodologies

Develop a risk methodology focused on consequences to CI/KR and federal networks that can be leveraged for risk decision making.

CIVILIAN CYBER SUPPORT: CYBERSECURITY MODERNIZATION



Cybersecurity Modernization

A robust understanding of the threat environment, and current engineering challenges, leads to the development of policy to drive modernization of cybersecurity services.

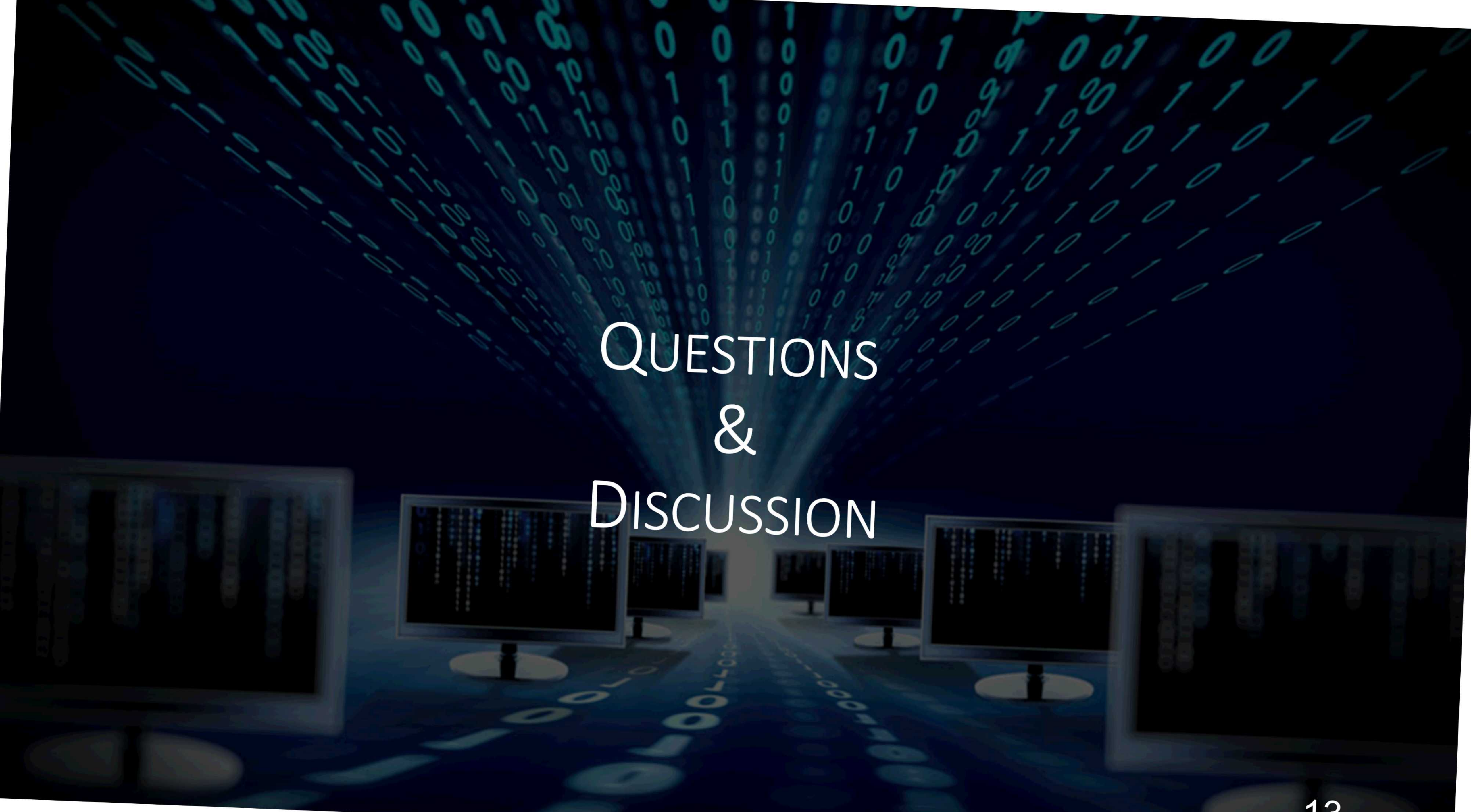
OPPORTUNITIES FOR PARTNERSHIP

Threat & Architecture Analysis

Enable smart investment decisions across the .gov environment through robust architecture and threat analysis.

Analysis of Emerging Trends

Understand the breadth of the emerging challenges, and develop mitigation strategies to maintain and evolve cybersecurity capabilities.



Questions & Discussion