

CISA | CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

OREGON CYBER RESILIENCE SUMMIT

CISA

Scott Buchanan
Acting Associate Director



CISA
CYBER+INFRASTRUCTURE

A RUSH TO THE BALL...



CISA ROLE

Cyber Threat Landscape

How Do we Fix the Cyber Gap?

Best Practices



CISA
CYBER+INFRASTRUCTURE





Cybersecurity and Infrastructure Security Agency (CISA)

VISION

Secure and resilient
infrastructure for the
American people.

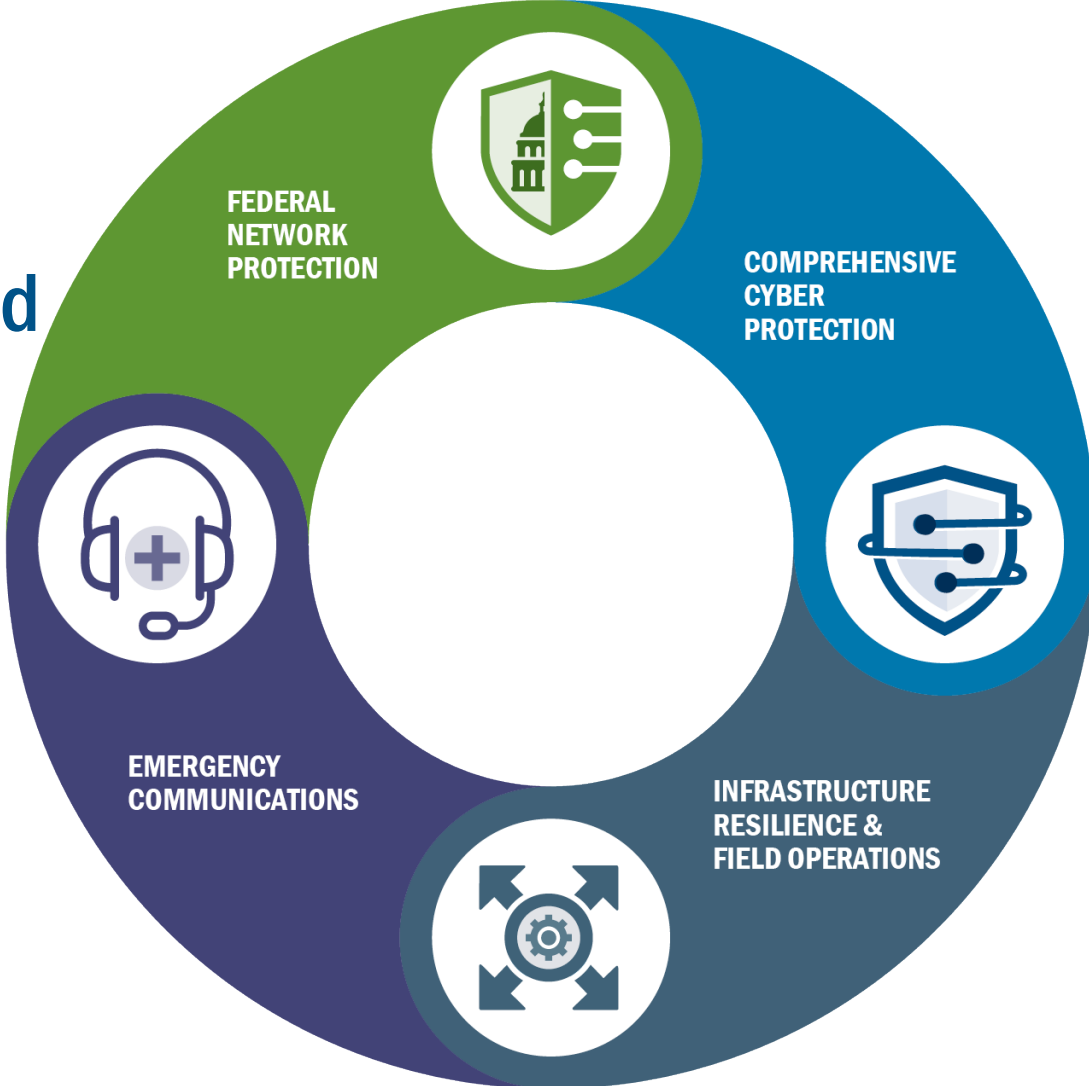
MISSION

Lead the Nation's efforts to
understand and manage risk
to our critical infrastructure.

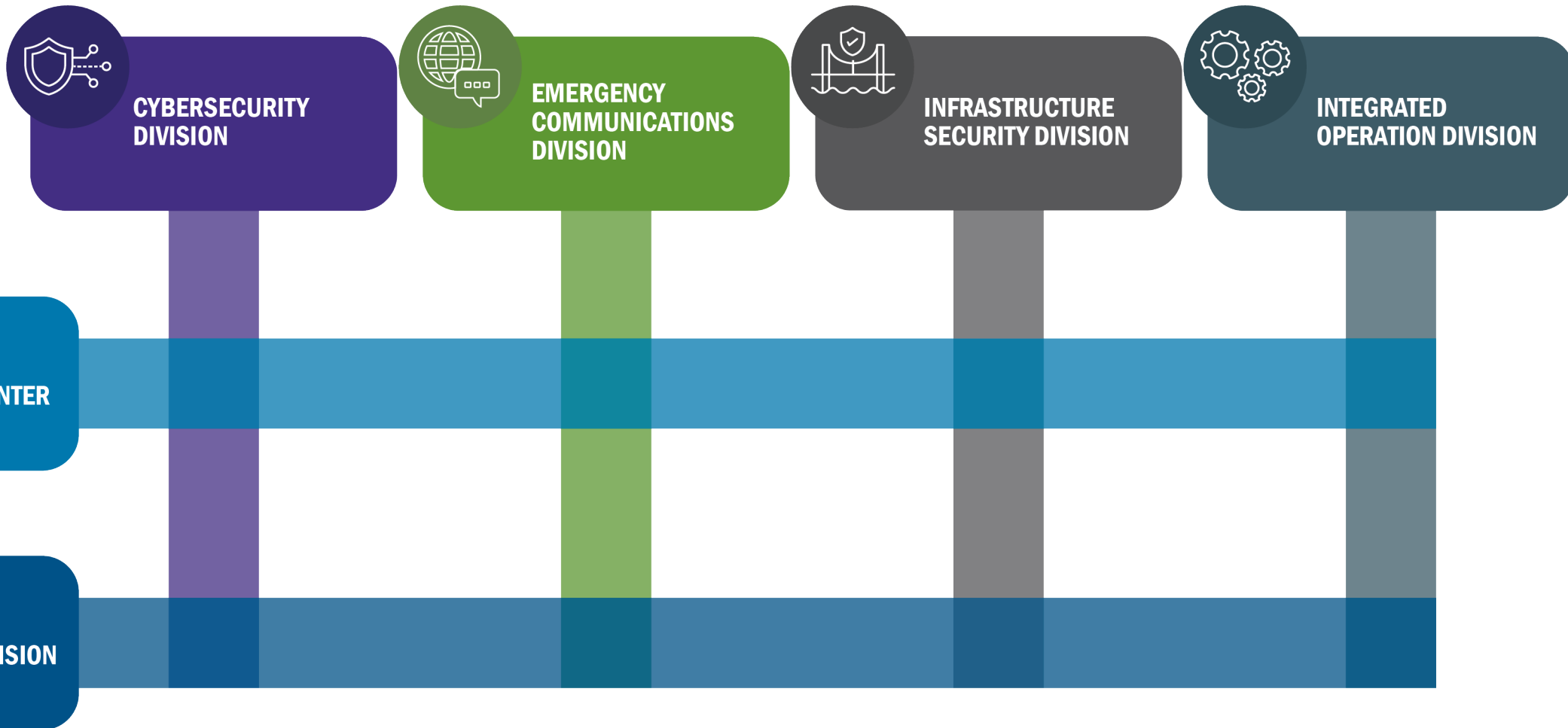
We are the Nation's Risk Advisors

CISA leads national risk management for cyber and physical infrastructure

-  PARTNERSHIP DEVELOPMENT
-  INFORMATION AND DATA SHARING
-  CAPACITY BUILDING
-  INCIDENT MANAGEMENT & RESPONSE
-  RISK ASSESSMENT AND ANALYSIS
-  NETWORK DEFENSE
-  EMERGENCY COMMUNICATIONS



CISA DIVISIONS



CISA
CYBER+INFRASTRUCTURE

“DEFEND TODAY, SECURE TOMORROW”

We lead the Nation’s risk management efforts by bringing together diverse stakeholders to collaboratively identify risks, prioritize them, develop solutions, and drive those solutions to ensure the stability of our national critical functions. As the nation’s risk advisor, CISA is unique in its position to partner with private industry, researchers, international governments, emergency responders, intelligence, defense, and other communities.

ENDS
OVERALL GOALS

GOAL 1



DEFEND TODAY
Defend against urgent
threats and hazards

GOAL 2



SECURE TOMORROW
Strengthen critical infrastructure
and address long-term risks

seconds

days

weeks

months

years

decades



CISA
CYBER+INFRASTRUCTURE

**WAYS
GENERAL METHODS**

Risk management planning,
governance, and execution

Risk visibility and analysis

Information sharing

Stakeholder engagement

Capacity building and technical services

Incident management and response

**MEANS
SPECIFIC RESOURCES**

Analysts, risk models, and technical alerts

Collaborative planning teams
and task forces

Policy and governance actions

Technical assistance teams
and security advisors

Deployed tools and sensors

Grants and operational contracts

Exercises and training



MISSION ESSENTIAL FUNCTIONS



INCIDENT MANAGEMENT:

Support management of physical, cyber and communications incidents in real time
Help mitigate impacts and reduce risks to critical systems



ANALYSIS:

Conduct analyses to recognize threats and vulnerabilities, identify countermeasures, and develop situational awareness



CAPACITY BUILDING:

Build capacity across all levels of government and the private sector to improve management of physical, cyber and communications risks



INFORMATION EXCHANGE:

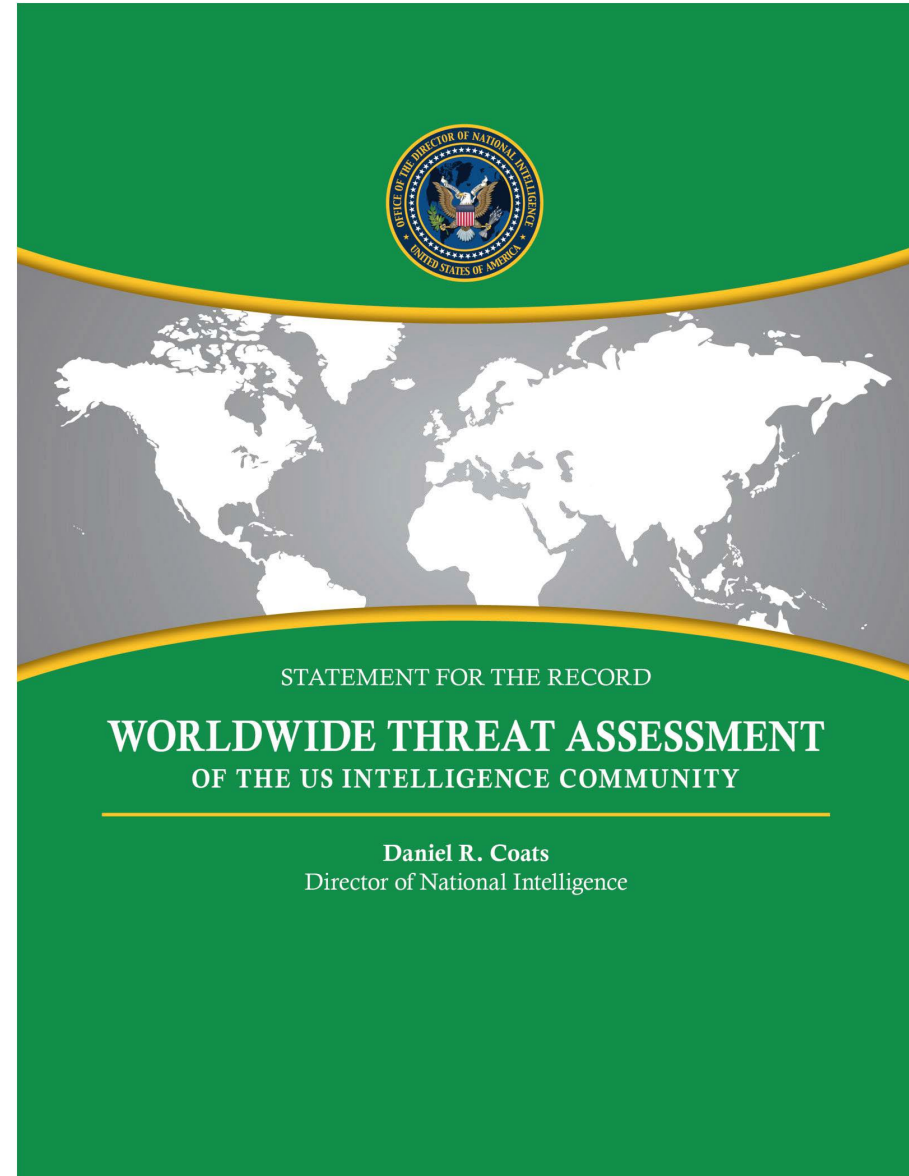
Share information about physical, cyber and communications risks to support stakeholder decisions and actions

Cyber

A Top Threat



CISA
CYBER+INFRASTRUCTURE



Today's Risk Landscape

America remains at risk from a variety of threats:



INSIDER THREAT



ACTS OF TERRORISM



CYBER ATTACKS



EXTREME WEATHER



PANDEMICS



ACCIDENTS OR TECHNICAL FAILURES

Cyber Interconnectivity

- **Complex cyber ecosystem of digital business**
- **North Korea targets financial institutions**
 - **Pattern for future – increase activity**
 - **High need to generate revenue**
 - **U.S. critical infrastructure disruptions**
 - **Healthcare, finance, government and emergency service sectors**



CISA
CYBER+INFRASTRUCTURE

- **ISC² reports Global Cybersecurity Workforce Shortage of 3 Million – 500,000+ in the US**
 - **Cyberseek cites over 300,000+ Cybersecurity openings in the US**
 - **Lack of a skilled workforce leaves Public and Private Sector organizations vulnerable to ever-increasing cyber threats**
- **So where should we focus?**

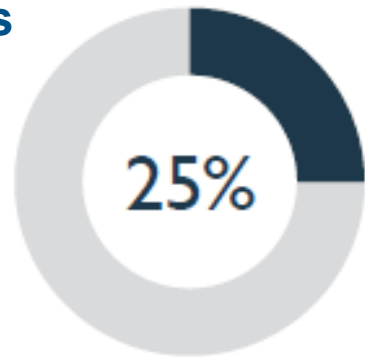


CISA
CYBER+INFRASTRUCTURE

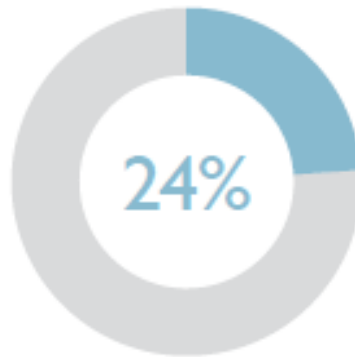
Problems within corporations themselves prevent a true focus on key cybersecurity initiatives

Top Challenges Preventing Focus on Key Cybersecurity Initiatives

IT & cybersecurity staff are the 1st to see budget cuts when issues arise



Low security awareness among end-users

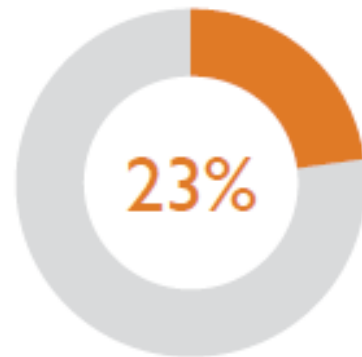


Not enough skilled cybersecurity professionals available

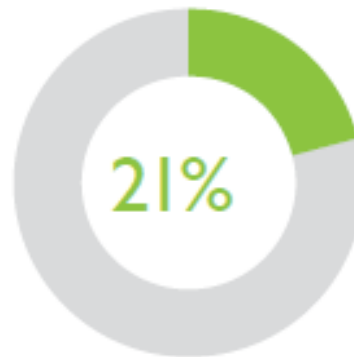


Inadequate funding

Corporate IT staff spends more than 54% of their time on cybersecurity issues



Too much data to analyze



Lack of management support/awareness

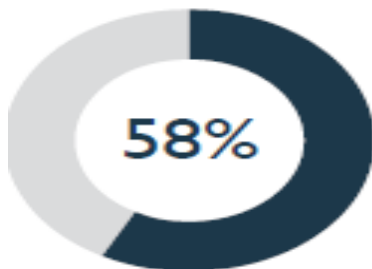


Top Needed Cybersecurity Areas of Expertise

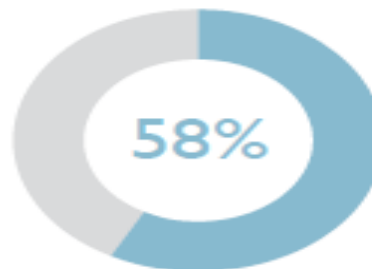
Showing % saying 'Critical'



Top Areas of Expertise Needed



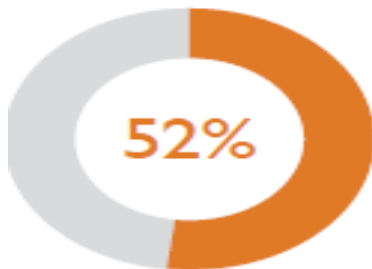
Security awareness



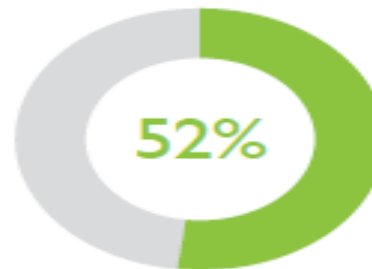
Risk assessment, analysis & management



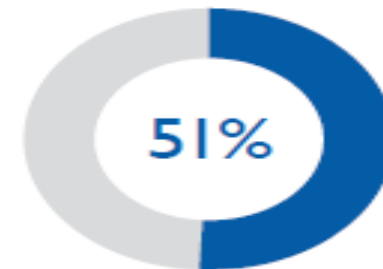
Security administration



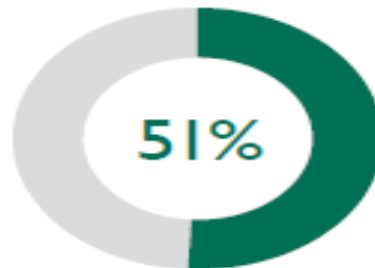
Network monitoring



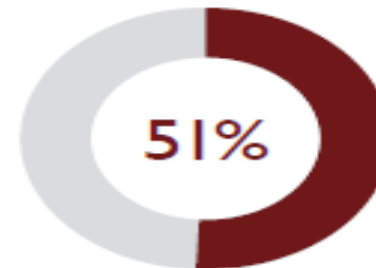
Incident investigation and response



Intrusion detection



Cloud computing security



Security engineering



CISA
CYBER+INFRASTRUCTURE

How to meet the need

- Curriculum developed that meets the needs – cloud, forensics, etc.
 - Too much managerial level – the need is for technical
- Labs – all cyber curriculum at the undergrad level need to incorporate labs both in residence and online in order to ensure technical proficiency
- Certificate Programs at the undergrad and Masters levels



CISA
CYBER+INFRASTRUCTURE

Best Practices

Leadership Must **OWN** the Issue

Be Prepared –
EXERCISE

Good Cyber Hygiene
– Blocking and
Tackling

Defend and
Continue to
Operate

Risk Management –
What Can I Accept?

+ Balance Security,
Mission and Privacy

Leverage
Relationships



CISA
CYBER+INFRASTRUCTURE

DO YOU FEEL LUCKY?



Source: <http://mentalfloss.com/article/75811/11-lucky-facts-about-dirty-harry>



CISA
CYBER+INFRASTRUCTURE