Topics

- Critical Infrastructure Market
- 16 Critical Infrastructure Sectors
- DHS Organizational Chart
- DHS National Critical Infrastructure Security and Resilience R&D Plan (CISR)
- National Protection and Programs Directorate
- Office of University Programs
- OUP and the Critical Infrastructure Resilience Institute at University of Illinois at Urbana-Champaign
- Upcoming Events
The critical infrastructure market is expected to increase from $87 billion in 2016 to $131 billion by 2021.

- Drivers: smart grids, IT spending, automation, integrated functioning of cloud and CIP, increase prevalence in cyber-attacks, and more efficient policy regulations and implementations.

An estimated **8.4 billion** devices are connected to the internet currently worldwide.

- Expected to increase to over **20 billion** devices by 2020.
- Drivers: fleet management in transportation, security/surveillance applications in government, inventory and warehouse management applications in retail and industrial asset management in manufacturing

(source: Mordor Intelligence, Gartner, Forrester)
Financial Drivers

• Cyber Security Market was valued at $52.05 billion in 2015. Projected to grow to $114.08 billion by 2024 with a compound annual growth rate (CAGR) of 9.1%.

• The airport, oil and gas, banking, and government segments will exhibit maximum growth during the forecast period. North America, Europe, APAC, and the Middle East (in the same order) will have the highest CAGRs during 2015 to 2024 (10.7%, 10.1%, 8.9%, and 7.1%).

• Increases in partnerships between traditional IT cyber security providers and infrastructure control system firms.

• Legislation.
Designation of 16 Critical Infrastructure Sectors

**Sector Specific Agency - DHS**
- Chemical Sector
- Commercial Facilities Sector
- Communications Sector
- Critical Manufacturing Sector
- Dams Sector
- Emergency Services Sector
- Government Facilities Sector
- Information Technology Sector
- Nuclear Reactors, Materials, and Waste Sector
- Transportation Systems Sector

**Sector Specific Agency - Non-DHS**
- Defense Industrial Base Sector
- Energy Sector
- Financial Services Sector
- Food and Agriculture Sector
- Healthcare and Public Health Sector
- Water & Wastewater Systems Sector
Since 2013, over **150 research** grants have been issued relating to critical infrastructure protection.

An estimated 2,500 companies and institutions are conducting research in critical infrastructure resiliency.
Organizational Structure

U.S. Department of Homeland Security
Policy Directive 21, Critical Infrastructure Security and Resilience (PPD-21) and Executive Order 13636, Improving Critical Infrastructure Cybersecurity

• The coordinated release of these two policies underscores commitment to integrating cyber and physical security and strengthening resilience across interrelated systems

• Requires DHS to provide a R&D plan that takes into account the evolving threat landscape, annual metrics, and other relevant information to identify priorities and guide R&D requirements and investments.

• 5 overarching R&D topics:
  • Develop the **foundational understanding** of critical infrastructure systems and systems dynamics;
  • Develop **integrated and scalable risk assessment** and management approaches;
  • Develop **integrated and proactive capabilities**, technologies, and methods to support secure and resilient infrastructure;
  • Harness the power of data sciences to create unified, **integrated situational awareness** and to understand consequences of action;
  • Build a crosscutting culture of CISR R&D collaboration.
DHS Critical Infrastructure Resilience
Mission Support

- DHS National Protection and Programs Directorate (NPPD)
  - **Office of Cyber and Infrastructure Analysis (OCIA)** – supports DHS implementation of PPD 21 which calls for integrated analysis critical infrastructure, and Executive Order 13636, identifying critical infrastructure where cyber incidents could have catastrophic impacts to public health and safety, the economy, and national security.
    - **OCIA Goals**
      - Provide innovative analysis that impacts key decisions affecting the security and resilience of critical infrastructure.
      - Establish strong collaborative relationships to ensure OICA’s analysis influences key decisions.
      - Products – Hurricane, Storms, Earthquakes, Drought, Flood, Cyber, and Modeling & Simulation, RRAP
  - The Office of Cybersecurity and Communications (CS&C) - responsible for enhancing the security, resiliency, and reliability of the nation's cyber and communications infrastructure.
    - safeguard federal government systems by reducing potential vulnerabilities, protecting against cyber intrusions, and anticipating future threats
DHS Science and Technology Directorate and University Outreach

Homeland Security Act 2002

The Under Secretary for Science and Technology shall have the responsibility for:

• “[establishing] … a coordinated, university-based system to enhance the Nation’s homeland security”
• “supporting United States leadership in science and technology”
• “merit review of research and development projects … and the dissemination of research conducted or sponsored by the Department”
The Office of University Program (OUP) streamlines access to the expertise of the Nation’s colleges and universities to address pressing homeland security needs:

• OUP makes it easy to tap into the intellectual power of America’s universities for homeland security research, development and education.

• DHS Components can access academic expertise to answer research questions, deliver technical solutions, and build a highly specialized workforce.

• OUP Program Managers provide individualized service to DHS Components and assist with finding needed R&D capabilities within OUP’s network of over 200 partner institutions.

• OUP offers established vehicles through which DHS Components and other partners can access the research and expertise found at the S&T Centers of Excellence.
Flexible and Creative Research Management

- High quality, practical R&D
- Professional development opportunities
- Full student funding
- Job/internship requirement
- Experienced senior staff
- Rigorous competitions
- Growing the homeland security workforce
- Research-Education-Transition Integration
- Risk tolerance
- Embedded researchers
- Builds infrastructure
- Long-term/rapid response research
- Experimental, continuous learning approach
- Creative management
- Faculty-staff exchange
- Easy access to COEs
- Funding vehicles
- "Constructs" COEs
- Balanced innovation/operational requirements
- Five-year term
- Annual funding
## COE Topic Alignment to DHS Missions

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Law Enforcement Investigations</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Arctic Domain Awareness</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Applied Quantitative Analysis</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Counterterrorism</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Countering Biothreats</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transportation Security and Screening</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maritime Domain Awareness</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Border Security, Trade and Immigration</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Infrastructure Protection and Resilience</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Natural Hazards and Resilience</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Focusing the CIRI Mission

**Key Considerations**

- Rapid expansion of the use of information and communications technologies (ICT) in all sectors has dramatically increased operational efficiency, reliability, and safety through improved control and situational awareness, while simultaneously creating new vulnerabilities and threat vectors.
- Reliance of all sectors on ICT increases the number, frequency, and type of interactions between cyber and physical systems.
- Humans and their actions or inactions complicate the identification and management of risk for organizations.
- Identification and management of risk for organizations

**CIRI R&D Themes**

- Insurance and Business Case for Resilience
- Macro and Micro Industrial Supply Chains
- Infrastructure Dependencies and Interdependencies
- Next generation communication

![CIRI Portfolio Breakdown](image)
CIRI Thematic Areas

Insurance and Business Case for Resilience
• Find economic ways to spread risk, primarily in cyber realms
• Technologies able to assess risk to standards acceptable by insurers
• Information sharing frameworks

Macro and Micro Industrial Supply Chains
• “micro” means intra-organization, “macro” means inter-organization
• Resilience issues in embedded systems
• Analysis of resiliency in business and policy context

Infrastructure Dependencies and Interdependencies
• “Situational awareness” of system dependencies/interdependencies
• Exploration of resilience governance issues
• Models of economic/social/physical impact of upsets

Communication
• Dependency of critical infrastructures on communication
• Mobile, Internet
Research vs. Technology and Capability Development?
What is the Appropriate Mix of ‘Project Types’?

The selection of ‘the types of projects’ is critical to establishing expectations for project outputs, potential of COE contributions to the field and articulating the development pathways.

What are the technical development steps for each type of project?

What are the intellectual property considerations for each grouping in order to realize the end goal?
Upcoming Events

• November 9th – DHS Critical Infrastructure Facebook Tech Talk
• November 16 – CIRI Mobile Communications Technical Discussion
• December 12-13th – Artificial Intelligence & Quantum Computing Workshop
• January 30-31st – DHS/CIRI Biannual Review