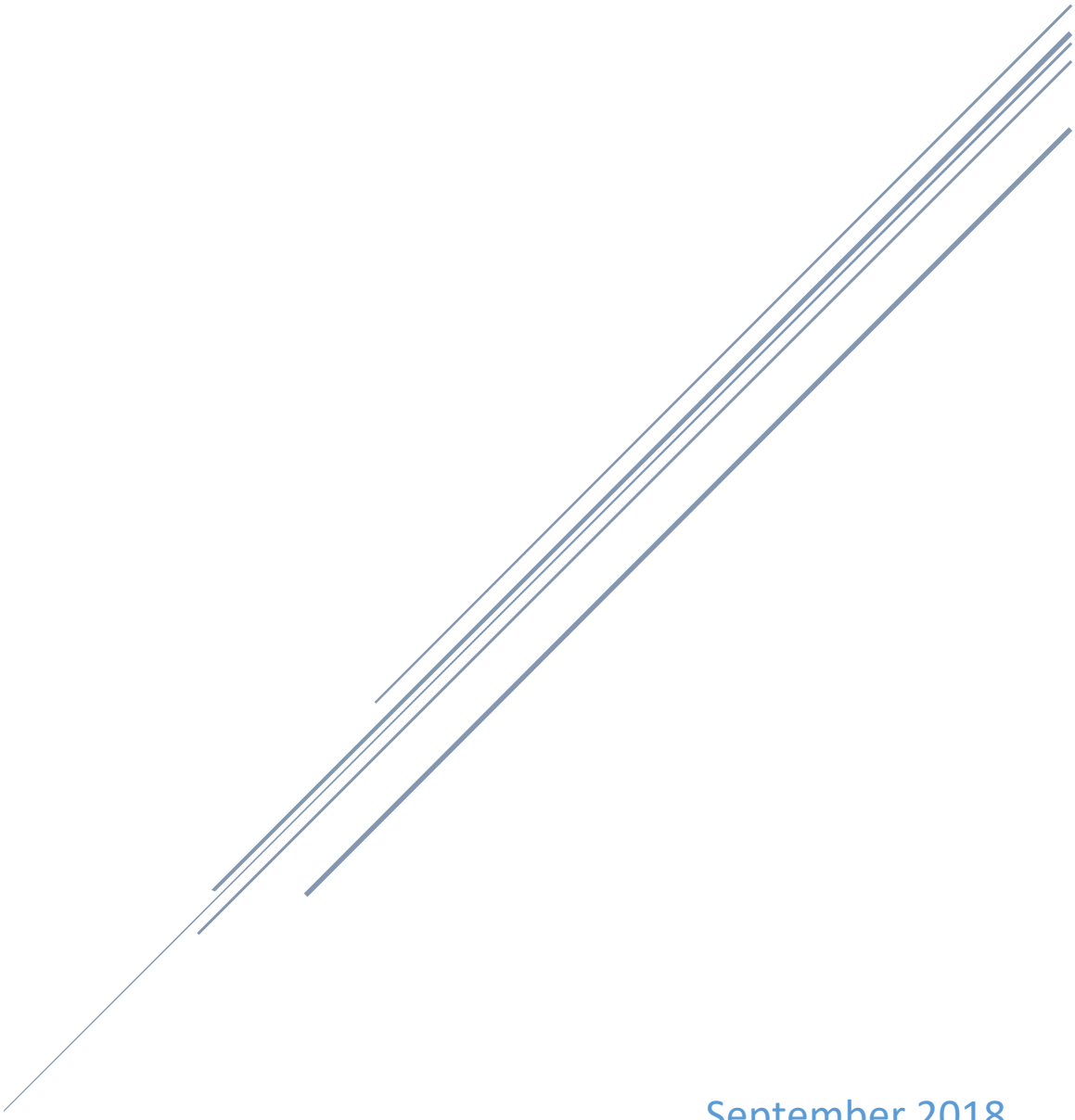
CYBER PRE- THRU POST- INCIDENT WORKING GROUP STRATEGIC PLAN

Chair: Major General Courtney Carr | Co-Chair: Dewand Neely



September 2018
Indiana Executive Council on Cybersecurity

Cyber Pre- thru Post- Incident Working Group Plan

Contents

Committee Members

Committee Members

	Name	Working Group Position	ECC Membership Type
	Dewand Neely	Co-Chair	Voting
	Courtney Carr (MG)	Co-Chair	Voting
	James Gordon	Advisory	Advisory
	Tim Winslow(COL)	Advisory	Advisory
	Jeff Hackett(COL)	Co-Chair Proxy	Voting Proxy
	David Tygart	Advisory	Advisory
Communications Sector - sub working group			
	Daniel J. Solero	Advisory	Voting Proxy
	Dave Skalon(LTC)	Voting	Advisory
Education Sector - sub working group			
	Andrew Korty	Voting	Advisory
	Matthew Etchison	Advisory	Advisory
	William Mackey	Voting	Advisory
	Chad Pollitt	Advisory	Advisory
	Darryl Togashi	Advisory	Advisory
	David Greer	Advisory	Advisory
Energy Sector - sub working group			
	Carl Cahill	Voting	Advisory
	Stanley Partlow	Advisory	Advisory
	Walter Grudzinski	Voting	Advisory
	Sarah Freeman	Advisory	Voting Proxy
Financial Sector - sub working groups			
	Seth Cooper	Voting	Advisory
	Owen LaChat	Voting	Voting
	Michael Servas	Advisory	Advisory
Government Law Enforcement - sub working group			
	Paul Dvorak	Advisory	Non-Voting
	John Davidson	Voting	Non-Voting
Government Services - sub working group			
	Thomas Vessely	Voting	Advisory
	James Haley	Advisory	Advisory
	Jeff Tucker	Advisory	Voting Proxy
	David Ehinger	Voting	Voting
Healthcare - sub working group			
	Frank Nevers	Voting	Advisory
	Mark Swearingen	Voting	Advisory
	David R. Day	Advisory	Advisory

Private Sector members			
	Landon Lewis	Advisory	Voting Proxy
	Ronald W. Pelletier	Advisory	Voting
	Nick Sturgeon	Voting	Advisory
	Kevin Mabry	Advisory	Advisory
	David Neel	Advisory	Advisory

Introduction

Introduction

With the signing of Executive Order 17-11 by Governor Eric J. Holcomb, the Indiana Executive Council on Cybersecurity (IECC) and its mission was continued. With the ever-growing threat of cyberattacks, the IECC has been tasked with developing and maintaining a strategic framework to establish goals, plans, and best practices for cybersecurity to protect Indiana's critical infrastructure. The IECC is comprised of twenty committees and working groups who worked together to develop a comprehensive strategic plan and implementation plans. This implementation plan is one of the twenty specific plans that make up the complete 2018 Indiana Cybersecurity Strategic Plan.

Executive Summary

Executive Summary

- **Research Conducted**
  - Each of our sector sub-groups was tasked to create a whitepaper specific to their area. The goal of these papers is to identify organic cyber capabilities and capability gaps within Indiana to better inform decision makers allowing us to prioritize and apportion limited resources to support the needs of the state's critical infrastructure.
  - Since October, we have been working to capture and examine other state cyber response plans in an effort to identify the best of the best to assist the IECC in creating our own plan. To date, we have reviewed and uploaded to Syncplicity 15 of the best state plans.
  - Finally, we have been exploring "GRIDEX-like" exercise for both the water and election sectors.

- **Research Findings**
  - Based on initial findings from our research, we see the need to look not only at the Energy sector but also into other sectors especially water and waste-water treatment. The main effort of most plans appears to be Energy Sector centric, specifically targeting the Electric sub-sector. While an attack on this sector would be far reaching it is also a sector with much regulation, governance, established response protocols and exercise programs. We propose that the State also look at other sectors to exercise during the planning phase. Two that come to mind are the water/wastewater and State election systems. Unlike Energy, where the loss of power is seen immediately, the contamination of a water source, assisted by a cyberattack, could go undetected and have a far-reaching impact.
  - According to the Indiana Utility Regulatory Commission, there are 555 water utilities in the State of Indiana. The Environmental Protection Agency (EPA) estimates of $14 billion capital investments required over the next 20 years to update its aging infrastructure. These costs will directly compete with capital investment into cybersecurity. Penetration testing is not the total answer: In a Pre Incident environment and the thousands of organizations spread across all sectors within Indiana there is simply not enough capability in Department of Homeland Security (DHS), National Guard or the Private sector to accommodate even a fraction of the need. Our efforts would be better served on "teaching them to fish" - outreach and training thru sector exercises is a better use of these limited resources and farther reaching than a penetration assessment alone.
  - We would recommend that the IECC also look strongly at developing outreach, training, and exercises for other Sectors.

- **Working Group Deliverables**
  - Exercise
  - Cyber Emergency Response Team (IN-CERT)
  - Gap Analysis
  - Penetration Testing

- **Additional Notes "Measures of Success Over Time:"**
    - One Year: Teams trained and available to conduct professional vulnerability assessments. Concepts developed to support outreach, training and exercises in various sectors.
    - Three Years: Established Cyber exercises in sectors other than Energy. For example; a water treatment tabletop at the Muscatatuck Urban Training Center using both virtual and physical plant to demonstrate vulnerabilities and train sector workforce. Considering an election system tabletop.
    - Five Years: Nationally recognized leader in critical infrastructure cyber defense preparedness, training, exercises and response.

Research

Research

1. **What has your area done in the last five years to educate, train, and prepare for cybersecurity?**
    a. As these questions are more geared towards specific Critical Infrastructure, we will discuss emergency response capabilities and how the National Guard can play a supporting role in support to cyber emergency response for the state. Over the past five years, there have been several exercises and table tops, GRIDEx and Crit-Ex to mention a few. Their focus was less of a whole of Government approach and more focused on a single critical infrastructures response needs. In any large-scale cyber incident, multiple agencies (DHS, IDHS, Indiana State Police (ISP), Federal Bureau of Investigation (FBI), etc.) will need to work together. Coordination over the past five years between these agencies and the National Guard was limited. To operate effectively in cyberspace, these agencies will require strong relationships and practiced coordination to ensure and effective response. Our goal going forward is to ensure we build strong partnerships.

2. **What (or who) are the most significant cyber vulnerabilities in your area?**
    a. The private sector owns and operates a vast majority of the nation's critical infrastructure; therefore, partnerships between State agencies in public and private sectors are essential to maintaining critical infrastructure, cybersecurity, and cyber resilience.

3. **What is your area's greatest cybersecurity need and/or gap?**
    a. Practiced partnerships among State and Federal Cyber response agencies.

4. **What federal, state, or local cyber regulations is your area beholden to currently**?
    a. The National Guard can operate in three distinct statuses with different authorities. Each status impacts when and how the National Guard can respond to cyberspace events.
    b. The first status is fully federalized. This is governed by Title 10, U.S. Code. In this status, the National Guard is the same as the Active Duty Army or Air Force. The authorities and policies governing this status are beyond the scope of this questionnaire.

c. The second status is federally funded, but state-controlled. This is Title 32 Status and is normally used to provide training for the federal mission. This is the one weekend a month, two weeks in the summer status that is typically associated with the National Guard. Current authorities restrict both the type and scope of cyberspace operations that the National Guard can perform under Title 32. The primary policies governing this area include Dep Sec Def Memo 16-002, known as the "CTAA Memo", and DTM 17-007, referred to as the "Cyber DSCA Memo." These policies limit any actions to Defensive Cyberspace Operations/Internal Defensive Measures (DCO/IDM). The policies allow for coordination and consultation, but do not allow the National Guard to be used in a Title 32 status off Department of Defense Networks (DODIN), absent specific circumstances. Additional authorities govern what and how information is stored and/or processed by the National Guard under Title 32. These include the Freedom of Information Act (FOIA), the Privacy Act, and the Health Insurance Portability and Accountability Act (HIPAA).
d. Finally, the National Guard may operate in State Active Duty. This is both State funded and controlled. In this status, National Guardsmen operate as if they were agents of the State. While the personnel are governed purely by state law in this status, any federal equipment they use still has restrictions attached. Additional restrictions, such as licensing agreements to restrict which systems and programs may be used in State Active Duty or off Department of Defense Networks. The use of federal intelligence equipment, systems, and personnel are limited to SECRET and below under the CTAA memo. The National Guard is also governed by state laws in the area, such as data breach disclosure laws, state privacy laws and state information disclosure laws.
e. In both Title 32 and State Active Duty status, there is no authority to perform any yes no actions other DCO/IDM. Any other actions, such as offensive actions or defensive response actions would potentially submit a guardsman to liability under federal criminal laws. These include the Computer Fraud and Abuse Act, 18 U.S.C. §1030 et seq.; the Wiretap Act, 18 U.S.C. §2511 et seq.; the Pen Trap/Trace Act 18 U.S.C. §3121 et seq.; and the Stored Communications Act 18 U.S.C. §2701 et seq.
f. In summary, under Title 32, the National Guard is limited to coordination and consultation, absent specific exceptions. When activated by the Governor under state active duty the National Guard can respond to cyberspace incidents but is still limited in what federal equipment and systems they may use or access. As with the civilian sector, certain actions, such as offensive cyberspace operations and defensive response actions are prohibited and may subject the individual to criminal penalties.

5. What case studies and or programs are out there that this Council can learn from as we proceed with the Planning Phase?

a. Other state plans and DHS sector papers.

6. What research is out there to validate your group's preliminary deliverables? This could be surveys, whitepapers, articles, books, etc. Please collect and document.

a. Other state plans have been collected by this working group and posted to the Syncplicity portal site.

b. To help better inform our decision-making process, white papers are being developed by our sub-groups on where best to focus assessments with the limited resources available. These documents will be uploaded to the Syncplicity portal when completed.
c. This information will culminate in an Executive summary of the State of Indiana Critical Infrastructure Cyber Preparedness and a Critical Infrastructure Priority Matrix that will drive our cyber focus in the years to come.

7. **What are other people in your sector in other states doing to educate, train, prepare, etc. in cybersecurity?**
    a. See state plans uploaded to Synplicity.

8. **What does success look like for your area in one year, three years, and five years?**
    a. <u>One Year</u>: Teams trained and available to conduct professional vulnerability assessments. Concepts developed to exercise various sectors developed.
    b. <u>Three Years</u>: Established Cyber exercises in sectors other than electric. For example: a Water Treatment tabletop at the Muscatatuck Urban Training Center using both virtual and physical plant to demonstrate vulnerabilities and train sector workforce. Considering an election system tabletop.
    c. <u>Five Years</u>: Nationally recognized leader in critical infrastructure cyber defense preparedness, training and exercises.

9. **What is the education, public awareness, and training needed to increase the State's and your area's cybersecurity?**
    a. N/A

10. **What is the total workforce in your area in Indiana? How much of that workforce is cybersecurity related? How much of that cybersecurity-related workforce is not met?**
    a. N/A

11. **What do we need to do to attract cyber companies to Indiana**?
    a. We think the question is how do we build a culture within Indiana that emphasizes the importance of investing in cybersecurity? Many smaller entities must balance capital investments into infrastructure versus cyber defense capabilities. A public information campaign and targeted outreach is one method to consider. Demonstrating vulnerabilities is another under consideration within the Pre thru Post Cyber Working Group.

12. **What are your communication protocols in a cyber emergency?**
    a. These are currently being developed to support other sector plans.

13. **What best practices should be used across the sectors in Indiana? Please collect and document.**
    a. Best practices are well established across the sectors. As stated earlier in the document we need to develop the cyber culture through state and sector sponsored outreach.

Deliverable: Exercise

Deliverable: Exercise

General Information

1. **What is the deliverable?**
    a. Cross Sector Critical Infrastructure Exercise that highlights critical deficiencies in the targeted sector(s) and exercise State emergency response.

2. **What is the status of this deliverable?**
    a. The completion of the Executive summary of the State of Indiana Critical Infrastructure Cyber Preparedness and a Critical Infrastructure Priority Matrix will be used to focus a State Exercise. This deliverable is currently at less than 5% pending the completion of the aforementioned documents.

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**
    ☐ Establish an effective governing structure and strategic direction.
    ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
    ☒ Strengthen best practices to protect information technology infrastructure.
    ☐ Build and maintain robust statewide cyber-incident response capabilities.
    ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
    ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
    ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**
    ☐ Research – Surveys, Datasets, Whitepapers, etc.
    ☐ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
    ☐ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
    ☒ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
    ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
    ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
    a. Improved awareness and cyber health of the targeted sector(s).
    b. Emergency response processes validated.

6. **What metric or measurement will be used to define success?**
    a. Exercise conducted.

7. **What year will the deliverable be completed?**
    a. 2020

8. **Who or what entities will benefit from the deliverable?**
    a. Critical Infrastructure, State Government agencies and Local governments

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. This type of service is also provided by Indiana Department of Homeland Security (IDHS), Indiana Office of Technology (IOT), and Indiana State Police (ISP).

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. Lesson learned may be shared with the public awareness and training working group to assist in focusing outreach efforts.

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. IDHS, IOT, ISP.

12. **Who should be main lead of this deliverable?**
    a. Pre thru Post Working Group & IDHS

13. **What are the expected challenges to completing this deliverable?**
    a. Funding - The state will have to work the funding if required.

Implementation Plan

14. **Is this a one-time deliverable or one that will require sustainability?**
    a. Ongoing/sustained effort

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
[No Response]				

Resources and Budget

15. Will staff be required to complete this deliverable?

a. Yes
b. **If Yes, please complete the following**:
    i. Unknown at this time, not counting Pre thru Post Working Group members.

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
Unknown at this time	Unknown at this time				

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.) Estimates only, nothing firm being too early in the process.

Resource	Justification/Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
Contractor	Run Exercise if large scale	$80,000[1]				

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. Strengthen best practices to protect high risk Critical Infrastructure and improved coordination with interagency response with State Emergency Response Operations.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. Improved awareness and cybersecurity posture.

19. What is the risk or cost of not completing this deliverable?

a. Continued risk and poor security posture.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. There is no measurable baseline. Success will be measured using After Actions Comments.

[1] This amount is rough order of magnitude and only used to identify potential costs. Once planning is initiated details of costs will be refined.

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

a. Yes
b. **If Yes, please list states/jurisdictions**
    c. Many states do have a central hub for its cybersecurity efforts as outlined in their State Cybersecurity Plans collected and posted for the IECC members in Syncplicity portal.
    d. Based on the direction this working group takes we will then draw about this information to build metrics.

22. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. Yes
b. **If Yes, please list states/jurisdictions**
    i. Some states are still in a drafting state for Cybersecurity Plans.
    ii. Based on the direction this working group takes we will then draw about this information to build metrics.

Other Implementation Factors

---

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. Lack of cooperation among agencies and availability of state funding.

24. Does this deliverable require a change from a regulatory/policy standpoint?

a. No

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. Currently this deliverable is designed as a one-time deliverable, therefore long-term design & support must be developed.

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. We are currently researching and developing initial concept; therefore, no outreach has been conducted regarding implementation at this time.

27. Can this deliverable be used by other sectors?

a. Yes
b. **If Yes, please list sectors**
    i. All

Communications

---

28. Once completed, which stakeholders need to be informed about the deliverable?

a. Unknown at this time.

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. Yes

30. What are other public relations and/or marketing considerations to be noted?

a. Unknown at this time.

Evaluation Methodology

Objective 1: The State of Indiana will develop and execute a Cross Sector Critical Infrastructure Cyber Exercise by December 2020.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Deliverable: Cyber Emergency Response Team (IN-CERT)

Deliverable: Cyber Emergency Response Team (IN-CERT)

General Information

1. **What is the deliverable?**
    a. Cyber Taskforce Enforcement Training

2. **What is the status of this deliverable?**
    a. Started

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**
    ☐ Establish an effective governing structure and strategic direction.
    ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
    ☐ Strengthen best practices to protect information technology infrastructure.
    ☒ Build and maintain robust statewide cyber-incident response capabilities.
    ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
    ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
    ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**
    ☐ Research – Surveys, Datasets, Whitepapers, etc.
    ☐ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
    ☐ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
    ☒ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
    ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
    ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
    a. To provide a training program for Indiana law enforcement who will also be a part of a state cyber taskforce that is able to respond to large-scale cyber emergencies.

6. **What metric or measurement will be used to define success?**
    a. Set up of training and with 20 number of law enforcement signing up for the training.

7. **What year will the deliverable be completed?**
    a. When funding is secured

8. **Who or what entities will benefit from the deliverable?**
    a. Law enforcement, public and private entities

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. N/A

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. Government Services

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. ISP, IDHS, and National Guard

12. **Who should be main lead of this deliverable?**
    a. ISP/IDHS

13. **What are the expected challenges to completing this deliverable?**
    a. Funding and establishing the new program.

Implementation Plan

14. **Is this a one-time deliverable or one that will require sustainability?**
    a. Ongoing/sustained effort

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Identify and price training	Group	100%	May 31	
Identify and price equipment	Group	100%	May 31	
Procure funding	Council Partners	0	TBD	
Identify personnel	Group	0	After funding procured	ISP to take lead
Begin training	Group	0	Within 12 months of funding procured	ISP to take lead

Resources and Budget

15. **Will staff be required to complete this deliverable?**
    a. No
    b. **If Yes, please complete the following**

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
N/A					

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

Resource	Justification/Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
Training and certifications	KSAs to respond to cyber emergency. Certifications needed to provide skilled fact and expert testimony.	$556,060.00	$100,000/year	grants		
Forensic tools	Needed for cyber emergency response	$100,672.20	$75,000/year	grants		

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. A rapid, forensically sound response to cyber emergency.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. Intercept commerce or public utility interruptions.

19. What is the risk or cost of not completing this deliverable?

a. Commerce and public utility interruptions. Failure to respond to cyber emergencies in a forensically sound manner and contamination of evidence such that bad actor attribution can't be accomplished.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. Rapid response to cyber emergencies in a manner in which the response follows adopted norms and protocols, while being done in a forensically sound manner and ensuring preservation of evidence.

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

a. No

22. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. No

Other Implementation Factors

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?
training availability

a. Inability to obtain grant funding.

24. Does this deliverable require a change from a regulatory/policy standpoint?

a. No

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. Continue funding along with continued training.

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. Chetrice Mosley

27. Can this deliverable be used by other sectors?

a. Yes
b. **If Yes, please list sectors**
    i. Any State law enforcement agency during the course of cybercrime investigations. Also provides a response to State prosecutors and courts for skilled fact and expert witnesses.

Communications

28. Once completed, which stakeholders need to be informed about the deliverable?

a. ISP, IDHS, and Indiana National Guard (INNG)

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. No

30. What are other public relations and/or marketing considerations to be noted?

a. None at this time.

Evaluation Methodology

Objective 1: Indiana State Police will develop and launch Indiana Cyber Emergency Response Team training program within 12 months of the Council partners securing an encumbered source of funding.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Deliverable: Gap Analysis

Deliverable: Gap Analysis

General Information

1. **What is the deliverable?**
    a. Gap Analysis – the identification of unfilled requirements within the state that presents a risk to cybersecurity.

2. **What is the status of this deliverable?**
    a. This requirement is on-going and has no start or end.

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**
    ☐ Establish an effective governing structure and strategic direction.
    ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
    ☒ Strengthen best practices to protect information technology infrastructure.
    ☐ Build and maintain robust statewide cyber-incident response capabilities.
    ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
    ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
    ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**
    ☒ Research – Surveys, Datasets, Whitepapers, etc.
    ☐ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
    ☐ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
    ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
    ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
    ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
    a. Better aligned limited resources to high risk.

6. **What metric or measurement will be used to define success?**
    a. Our ability as a state to identify and then fund and fill critical gaps. This effort will not stop as it must be continually evaluated to identify new risks and gaps that need addressing.

7. **What year will the deliverable be completed?**
    a. This line of effort is on-going and has no definitive end date.

8. **Who or what entities will benefit from the deliverable?**
    a. Critical Infrastructure, State Government agencies and Local governments

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. This type of service is also provided by IDHS, IOT, ISP.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. As gaps are identified and evaluated, other groups will be brought into the process.

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. This depends on the gap being considered. In many cases IDHS, IOT, and/or ISP.

12. **Who should be main lead of this deliverable?**
    a. Pre thru Post Working Group

13. **What are the expected challenges to completing this deliverable?**
    a. Funding - The state will have to work the funding.

Implementation Plan

14. **Is this a one-time deliverable or one that will require sustainability**?
    a. It's a sustained effort because gaps must be continually identified. Each gap identified is a one-time deliverable to remediate it.

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
N/A				

Resources and Budget

15. **Will staff be required to complete this deliverable?**
    a. Yes
    b. **If Yes, please complete the following**
        i. Unknown at this time.

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
N/A					

16. **What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)**
    a. Unknown at this time.

Resource	Justification/ Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
N/A						

Benefits and Risks

17. **What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)**
    a. Risks are mitigated.

18. **How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?**
    a. Costs and risk are evaluated for each identified gap and handled under separate documentation.

19. **What is the risk or cost of not completing this deliverable?**
    a. Identified the risks that are not mitigated.

20. **What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?**
    a. Success and metrics are evaluated for each identified gap and handled under separate documentation.

21. **Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?**
    a. No

22. **Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?**
    a. No

Other Implementation Factors

23. **List factors that may negatively impact the resources, timeline, or budget of this deliverable?**
    a. Unknown at this time

24. **Does this deliverable require a change from a regulatory/policy standpoint?**
    a. Unknown at this time

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. Unknown at this time

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. N/A

27. Can this deliverable be used by other sectors?

a. N/A, each identified gap is handled under separate documentation.

Communications

---

28. Once completed, which stakeholders need to be informed about the deliverable?

a. Dependent on each gap identified.

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. Potentially

30. What are other public relations and/or marketing considerations to be noted?

a. Unknown at this time.

Evaluation Methodology

Objective 1: IECC Cyber Pre thru Post Incident Working Group will complete a comprehensive gap analysis of identified high risk critical infrastructure sectors by August 2018.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Objective 2: IECC Cyber Pre thru Post Incident Working Group provide recommendations based on a comprehensive gap analysis of identified high risk critical infrastructure sectors by December 2018.

Type: ☐ Output ☒ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☒ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Deliverable: Cyber Assessments

Deliverable: Cyber Assessments

General Information

1. **What is the deliverable?**
    a. Cyber assessments will be developed and delivered along two distinct lines: 1) Developing partnerships to support and augment local/state government entities cyber assessment requirements. 2) Developing baseline risks for an identified Indiana critical infrastructure structure to inform a cyber exercise.

2. **What is the status of this deliverable?**
    a. In-progress; 25% complete

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**
    ☐ Establish an effective governing structure and strategic direction.
    ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
    ☒ Strengthen best practices to protect information technology infrastructure.
    ☐ Build and maintain robust statewide cyber-incident response capabilities.
    ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
    ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
    ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**
    ☐ Research – Surveys, Datasets, Whitepapers, etc.
    ☐ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
    ☐ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
    ☒ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
    ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
    ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
    a. Independent assessment of network vulnerabilities.

6. **What metric or measurement will be used to define success?**
    a. Ability to sustain 2 tests per month.

7. **What year will the deliverable be completed?**
    a. To start no later than (NLT) Dec 2018

8. **Who or what entities will benefit from the deliverable?**
    a. Initially state government agencies and then local governments

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. This type of service is also provided by DHS.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. Lesson learned may be shared, without identification of agency, with the public awareness and training working group to assist in focusing outreach efforts.

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. IDHS

12. **Who should be main lead of this deliverable?**
    a. Pre thru Post Working Group

13. **What are the expected challenges to completing this deliverable?**
    a. Funding - State active duty fund will be required in order for Nation Guard personnel to work on non-Department of Defense (DoD) networks.

Implementation Plan

14. **Is this a one-time deliverable or one that will require sustainability?**
    a. Ongoing/sustained effort

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Develop Concept	INNG	25%	TBD	Personnel are mobilized and will not be available until late summer 2018 to start developing this program.

15. Will staff be required to complete this deliverable?

a. Yes
b. **If Yes, please complete the following**
   i. Costs are based on two weeks (ten days) with four personnel per day.

Assessment Costs: (personnel)
1 - O4 Cyber Team Chief
1 - W3 Cyber Tech lead
1 - E8 Cyber Operators
1 - E7 Cyber Operators

Assessment/PEN Costs						
		day		*week*		*month*
a. Pay	$	898.40	$	4,491.99	$	19,315.56
b. BAH	$	74.70	$	373.50	$	1,606.05
c. Lodging and Rations	$	162.00	$	810.00	$	3,483.00
d. BAS	$	41.46	$	207.31	$	891.42
GRAND TOTAL	**$**	**1,176.56**	**$**	**5,882.80**	**$**	**25,296.03**

Time Line: (typically two weeks for a basic assessment or penetration (PEN) test of a medium to small organization.
- Five days (collection of assets and resources information, objectives identified)
- 2-3 days (Hands-on assessment PEN testing)
- 2-3 days (Findings report publish and reviewed with the customer, best practices provided)

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
see above		Cyber CPT	State Active Duty	none	

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

Resource	Justification/Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
Non DoD equipment	Use of Federal funding maybe disallowed	$40,000	$5,000	State	none	

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. Under current definitions of U.S. Title 10 law and Department of Defense Directives the use of federally funded equipment for the National Guard could be utilized to support the Governor only by those Service Members while serving in a "State Active Duty" status. Any cyber response team, existing of non-military members, would require equipment procured outside of Federal channels, e.g. State or self-funded. Estimates in the table above are the rough order of magnitude costs to the State if the purchase of basic cyber assessment equipment sets were required.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. Not measurable

19. What is the risk or cost of not completing this deliverable?

a. Status quo, no improvement in cyber readiness.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. Success will be measured by executing one (1) assessment per month starting 2019 and dependent on the State providing funding.

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

a. Yes
b. If Yes, please list states/jurisdictions
    i. Ohio, Washington, Virginia

22. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. No

Other Implementation Factors

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. Willingness of State agencies or Critical Infrastructure Sector to allow assessments. Lack of state funding.

24. Does this deliverable require a change from a regulatory/policy standpoint?

a. No

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. To truly sustain this for the state would require fulltime personnel as National Guard soldiers must take leave from their full-time jobs to conduct these tests. We have no full-time personnel on staff.

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. [No Response]

27. Can this deliverable be used by other sectors?

a. [No Response]
b. **If Yes, please list sectors**
    i. N/A

Communications

---

28. Once completed, which stakeholders need to be informed about the deliverable?

a. On-going

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. Yes

30. What are other public relations and/or marketing considerations to be noted?

a. Unknown at this time.

Evaluation Methodology

Objective 1: Indiana National Guard will develop a Local/State Government Cyber Assessment Program by December 2018.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Objective 2: Indiana National Guard will conduct Cyber Assessment for State critical infrastructure entities by December 2019.

Type: ☐ Output ☒ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Supporting Documentation

Supporting Documentation

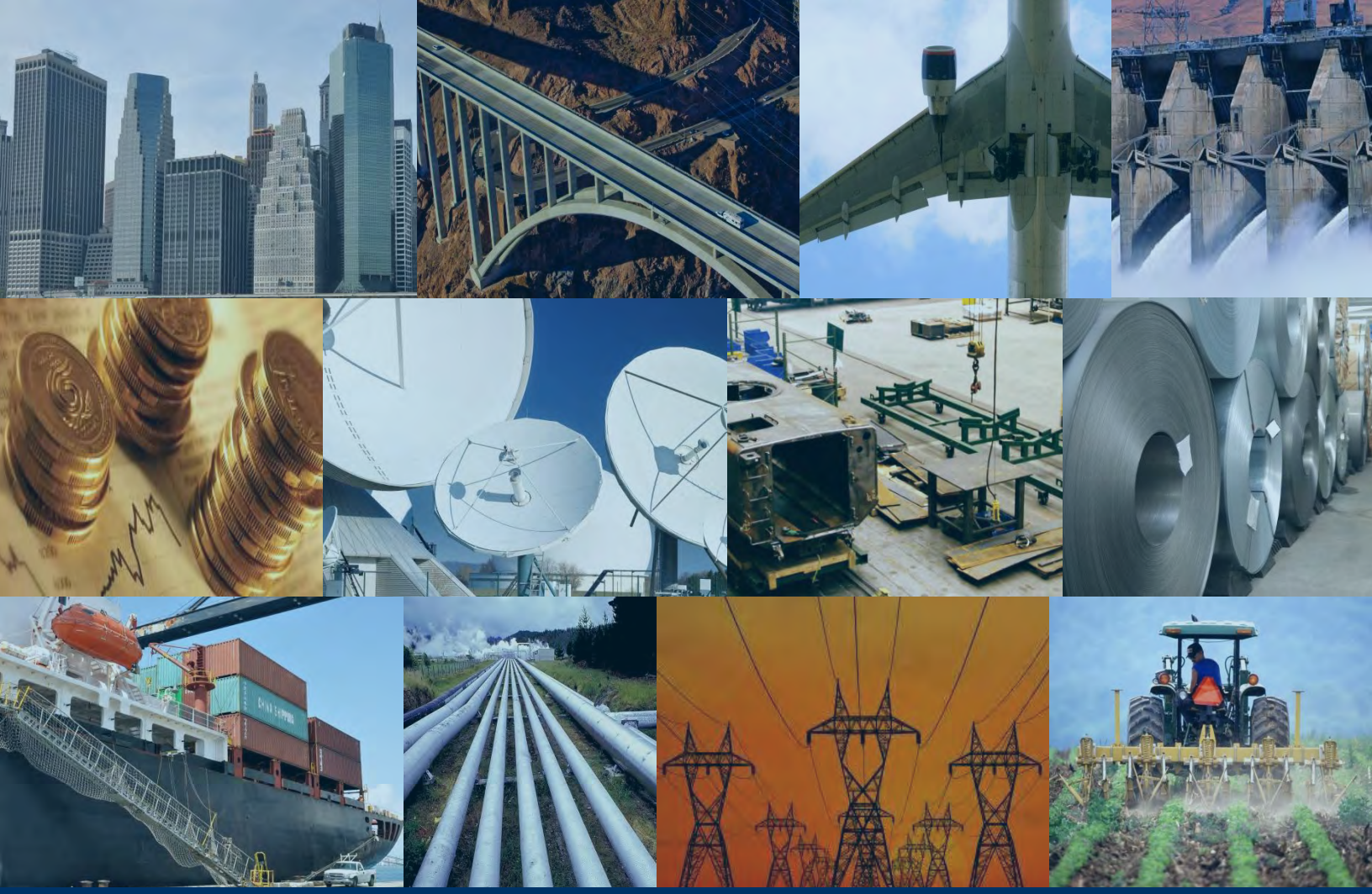
This section contains all of the associated documents that are referenced in this strategic plan and can be used for reference, clarification, and implementation details.

- Department of Homeland Security (DHS) Sector Risk Snapshots
- IECC Cyber Vulnerabilities Whitepaper – Communications Sector
- IECC Cyber Vulnerabilities Whitepaper – Energy Sector
- IECC Cyber Vulnerabilities Whitepaper – Water and Wastewater Sector
- IECC Pre- through Post-Incident White Paper – Education Sector
- Indiana National Guard (INNG) State Cyber Baseline Survey Results

Department of Homeland Security (USDHS)

Sector Risk Snapshots

May 2014



Sector Risk Snapshots

May 2014

Homeland Security

Sector Risk Snapshots

Introduction

Ensuring the security and resilience of critical infrastructure—those assets, systems, and networks that underpin American society—is essential to the Nation's security, public health and safety, economic vitality, and way of life. Managing risks to critical infrastructure requires an integrated approach across the whole-of-community to:

- Identify, deter, detect, and prepare for threats and hazards to the Nation's critical infrastructure;
- Reduce vulnerabilities of critical assets, systems, and networks; and
- Mitigate the potential consequences to critical infrastructure of incidents or adverse events that do occur.

Mission

Strengthen the security and resilience of the Nation's critical infrastructure by managing physical and cyber risks through the collaborative and integrated efforts of the critical infrastructure protection community.

National Infrastructure Protection Plan (NIPP), 2013

Presidential Policy Directive 21 (*PPD-21)* on *Critical Infrastructure Security and Resilience*, builds on the extensive work done to date to protect critical infrastructure, and identifies 16 critical infrastructure sectors:

- Chemical
- Commercial Facilities
- Communications
- Critical Manufacturing
- Dams
- Defense Industrial Base
- Emergency Services
- Energy
- Financial Services
- Food and Agriculture
- Government Facilities
- Healthcare and Public Health
- Information Technology
- Nuclear Reactors, Materials, and Waste
- Transportation Systems
- Water and Wastewater Systems

This compendium of Sector Risk Snapshots provides a brief overview and risk profile of the 16 critical infrastructure sectors, the Education, Electric, and Oil and Natural Gas Subsectors, and the seven Transportation Systems Modes. The Snapshots provide an introduction to the diverse array of critical infrastructure sectors, touching on some of the key threats and hazards concerning the sectors, and highlighting the common, first-order dependencies and interdependencies between sectors. The Snapshots are intended to serve as quick reference aids for homeland security partners, particularly State and local partners, and fusion center analysts, and each Snapshot includes a list of resources that partners can go to for more comprehensive sector information.

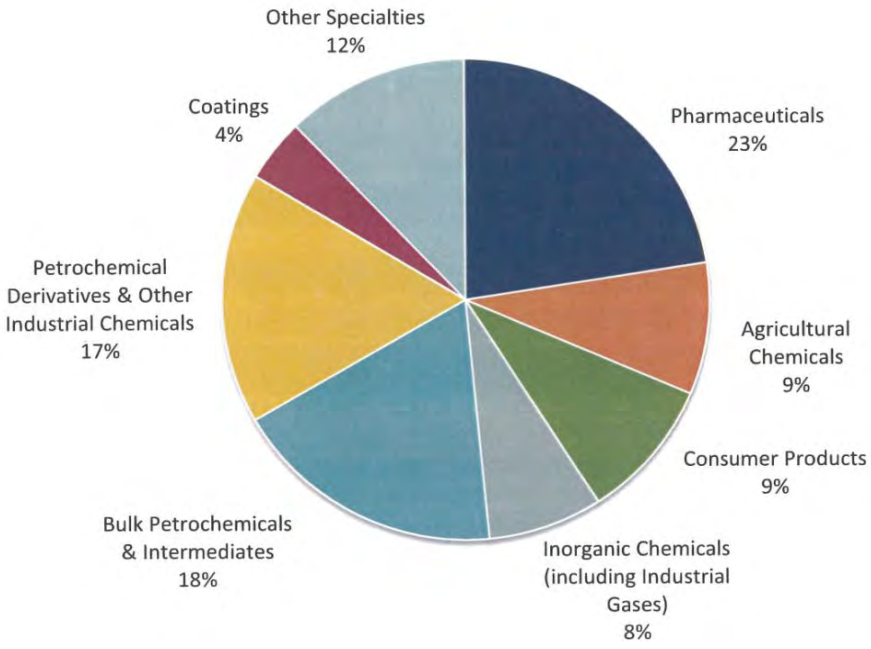
Prepared by the DHS Office of Cyber and Infrastructure Analysis (OCIA). For more information, contact OCIA at OCIA@hq.dhs.gov or visit our Website at www.dhs.gov/office-cyber-infrastructure-analysis.

Homeland Security

Chemical Sector Sector Risk Snapshot

Figure 1: Approximately 13,500 Chemical Manufacturing Facilities are in the U.S., owned by more than 9,000 Companies. *Source: Environmental Protection Agency (EPA, 2011)*

Figure 2: Global Chemical Shipments by Segment (as a percent of total shipments)



Chemical Sector Overview

- **The Chemical Sector is an integral component of the U.S. economy, employing nearly 1 million people, and earning annual revenues between $600 and $700 billion.**
- **Chemical Sector facilities typically belong to one or more of four key functional areas: (1) manufacturing plants, (2) transport systems, (3) warehousing and storage systems, and (4) chemical end users. In addition, companies may operate facilities across multiple functional areas, for example, a chemical manufacturer may also own a trucking and distribution operation.**
- **While the key functional areas primarily describe their physical characteristics and activities, each of the four functional areas depends on cybersystems for a variety of purposes, including operating manufacturing processes, tracking inventory, and storing customer information.**
- **As one of the oldest industries in the country, the chemical industry has a long history of resilience, based on the sector's ability to adapt to, prevent, prepare for, and recover from all hazards, including natural disasters, fluctuating markets, or a change in regulatory programs.**
- **To maintain operational resilience, successful businesses identify their critical dependencies and interdependencies and develop appropriate strategies to manage critical systems disruptions, should they occur.**
- **The DHS Chemical Facility Anti-Terrorism Standards (CFATS) program identifies and regulates high-risk chemical facilities to ensure they have security measures in place to reduce the risks associated with these chemicals. Upon review of more than 44,000 preliminary assessments from facilities with chemicals of interest, 4,275 facilities are now covered by CFATS (DHS, 2013).**

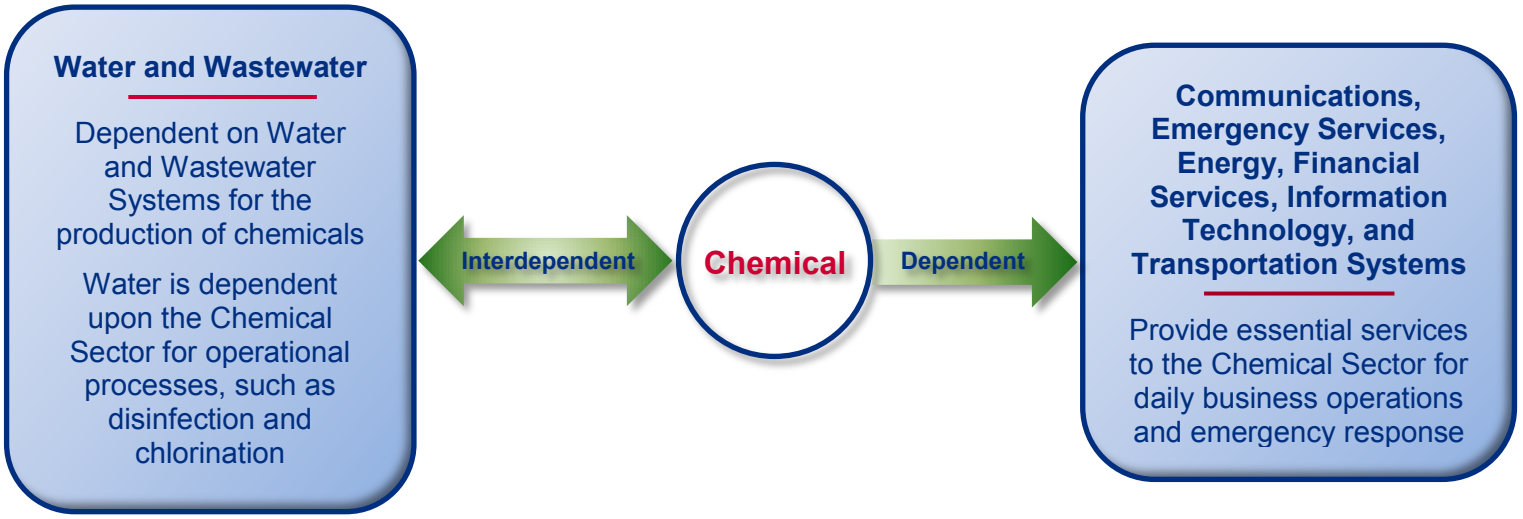
Threats and Hazards of Significant Concern

- **Cyberthreats**
  - The Chemical Sector is vulnerable to the threat of malicious actors physically or remotely manipulating network-based systems designed to control chemical manufacturing processes or process safety systems.
  - The physical disruption inflicted upon industrial assets in 2010 by the Stuxnet worm is evidence that control systems are vulnerable to increasingly destructive attacks and that the U.S. critical infrastructure may face cyberattacks of increasing sophistication.
- **Insider Threat**
  - While a facility can increase its physical security measures substantially, insiders with access who choose to intentionally cause harm will continue to contribute risk to the Chemical Sector. (CFATS, 2010, www.federalregister.gov/articles/2010/04/13/2010-8312/national-protection-and-programs-directorate-chemical-facility-anti-terrorism-standards-personnel#h-10)
  - Factors that improve management of this risk include greater cooperation and less competition among owners and operators within the sector and relatively higher cooperation between owners and operators and their workforces. (NIAC, *Insider Threat*, 2008, www.dhs.gov/xlibrary/assets/niac/niac_insider_threat_to_critical_infrastructures_study.pdf)
- **Natural Disasters and Accidents**
  - Natural disasters and accidents contribute to the ongoing risk of exposing the environment and the population to chemicals.
  - Accidents such as the 2013 West Fertilizer Company explosion—an ammonium nitrate explosion that resulted in 15 deaths, over 160 injuries, and more than 150 damaged or destroyed buildings in West, Texas—demonstrate the significant potential consequences of incidents involving harmful chemicals.

For More Information

- Sector-Specific Agency: DHS, Office of Infrastructure Protection, chemicalsector@hq.dhs.gov and www.dhs.gov/chemical-sector
- DHS, *National Risk Pro*file, OCIA@hq.dhs.gov.
- National Infrastructure Protection Plan, www.dhs.gov/national-infrastructure-protection-plan
- Maritime Transportation Security Act of 2002, www.tsa.gov/assets/pdf/MTSA.pdf
- Chemical Facility Anti-Terrorism Standards (CFATS), www.dhs.gov/chemical-facility-anti-terrorism-standards

Figure 3: Common, First-order Dependencies and Interdependencies of the Chemical Sector



May 2014

Homeland Security

Prepared by the DHS National Protection and Programs Directorate
Office of Cyber and Infrastructure Analysis (OCIA)
Questions or comments should be directed to OCIA@hq.dhs.gov

Homeland Security

Commercial Facilities Sector
Sector Risk Snapshot

Critical Infrastructure Protection Issues

- Owners and operators are responsible for the day-to-day protection of commercial facilities, in close cooperation with local law enforcement.
- The Government has various programs and efforts to support the protection of commercial facilities. Activities include providing timely threat indications and warnings, and working with organizations to identify vulnerabilities and mitigate risks through protective programs and training.
- Given the national-level visibility and potential human and economic consequences of prominent commercial facilities, it is important for the Federal Government and the Commercial Facilities Sector to work together to ensure the protection of the Nation's prominent business centers and public gathering places.

The Department of Homeland Security oversees the implementation and execution of protective measures programs across the Commercial Facilities Sector. Some of the programs currently underway include:

Risk Self-Assessment Tool (RSAT): Delivers an all-hazard analysis of a facility's current risk level and offers options for consideration on reducing and managing potential vulnerabilities.

Protective Security Advisor (PSA) Program: PSAs are critical infrastructure protection and vulnerability assessment specialists with a wealth of anti-terrorism and security experience deployed across the U.S.

Bomb-making Materials Awareness Program (BMAP): Assist commercial retailers, commercial service providers, and chemical distributers/wholesalers in identifying suspicious purchases of materials used in home-made explosive or improvised explosive device manufacturing.

Protective Measures Guides: An overview of possible threats, vulnerabilities, and protective measures designed to assist facility owners and operators in planning and managing security specific to their venue to maintain a safer environment for guests and employees.

Suspicious Activity Videos: Designed to raise the level of awareness for hotel and retail employees by highlighting the indicators of suspicious activity.

Commercial Facilities Sector Overview

- **Commercial Facilities Sector operates on the principle of open public access, meaning that the general public can move freely throughout these facilities without the deterrent of highly visible security barriers.**
- **The majority of the facilities in this sector are privately owned and operated, with minimal interaction with the Federal Government and other regulatory entities.**
- **The Commercial Facilities Sector consists of the following eight subsectors:**

1. **Public Assembly (e.g., arenas, stadiums, aquariums, zoos, museums, convention centers);**
2. **Sports Leagues (e.g., professional sports leagues and federations);**
3. **Gaming (e.g., casinos);**
4. **Lodging (e.g., hotels, motels, conference centers);**
5. **Outdoor Events (e.g., theme and amusement parks, fairs, campgrounds, parades);**
6. **Entertainment and Media (e.g., motion picture studios, broadcast media);**
7. **Real Estate (e.g., office and apartment buildings, condominiums, mixed-use facilities, self-storage); and**
8. **Retail (e.g., retail centers and districts, shopping malls).**

Threats and Hazards of Significant Concern

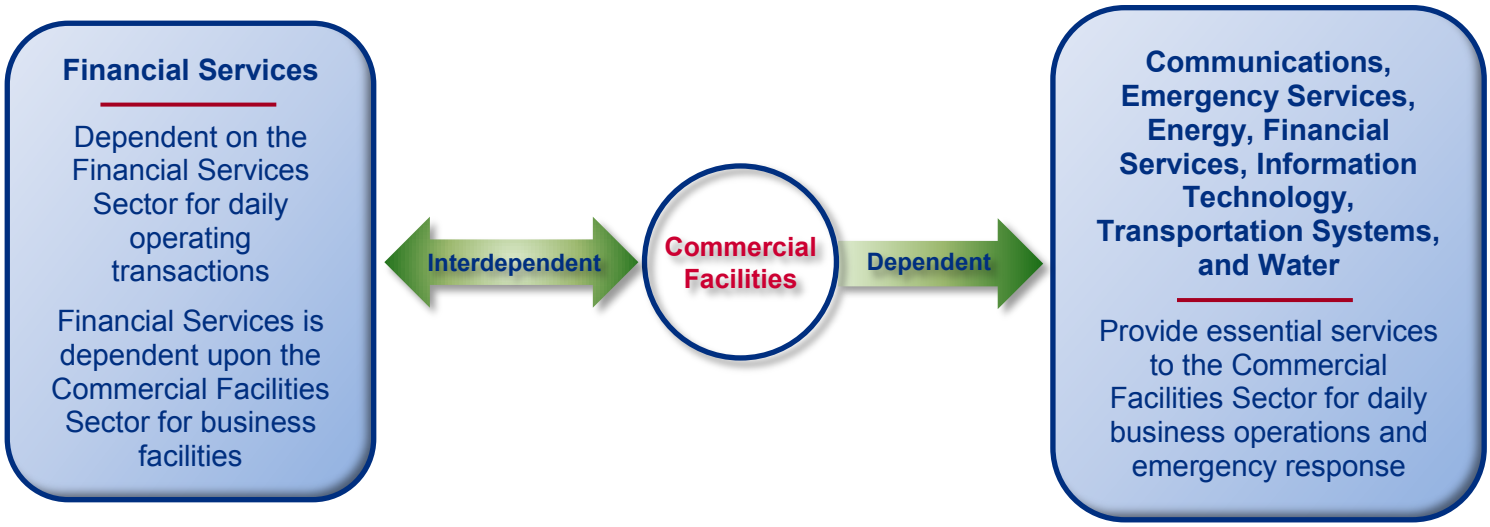
The Commercial Facilities Sector operates through a principle of open public access, which can increase the vulnerability to many types of attack methodologies. In addition, many Commercial Facilities Sector venues are highly recognizable, thus increasing the potential attractiveness to an adversary. These characteristics increase the risk to the Commercial Facilities Sector.

- **Bombings**
  - The adversary has expressed interest, and has a history of the use of explosive attacks against the Commercial Facilities Sector.
  - This attack methodology has the potential for creating mass casualties.
- **Active Shooter**
  - While a small arms attack may produce fewer casualties then an explosive attack, this attack methodology requires fewer resources and planning.
  - As in the case with bombings, the sector's open public access and population density make commercial facilities vulnerable to small arms attacks, resulting in an increased risk to the sector.
- **Chemical, Biological, Radiological (CBR) Attacks**
  - Some terrorist organizations have expressed interest in acquiring and using CBR weapons. Given the nature of mass gathering, and open public access of the Commercial Facilities Sector, there are unique vulnerabilities to either the distribution of CBR materials through ventilation systems or through liquid distribution in an open arena type environment.
  - Outdoor facilities, such as public assemblies or sporting events, are also at risk. Al-Qaeda has previously expressed interest in obtaining crop dusters, which could be used to disseminate aerosolized CBR agents over large areas and gatherings.

For More Information

- Sector-Specific Agency: DHS, Office of Infrastructure Protection, www.dhs.gov/commercial-facilities-sector
- DHS, *National Risk Profile,* OCIA@hq.dhs.gov.
- Commercial Facilities Resources: www.dhs.gov/commercial-facilities-resources

Figure 1: Common, First-order Dependencies and Interdependencies of the Commercial Facilities Sector



May 2014

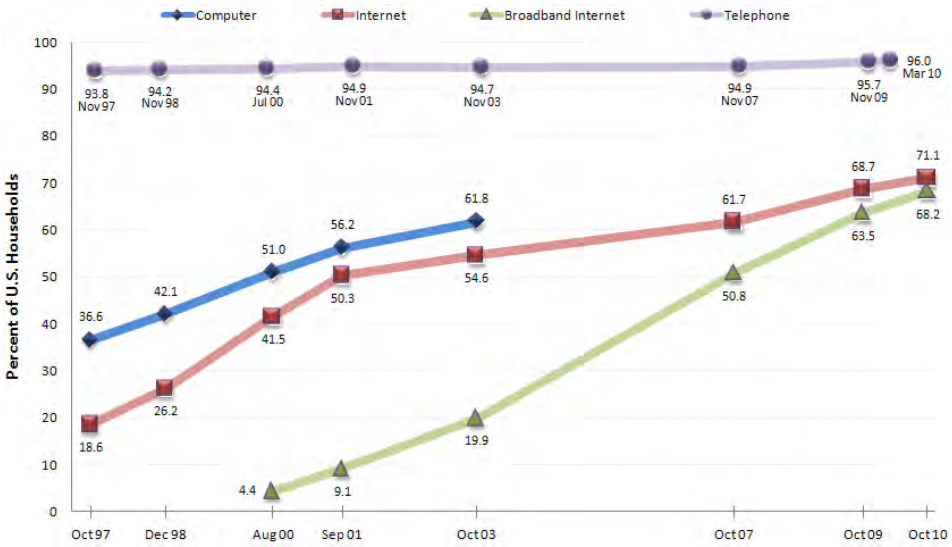
Homeland Security

Prepared by the DHS National Protection and Programs Directorate
Office of Cyber and Infrastructure Analysis (OCIA)
Questions or comments should be directed to OCIA@hq.dhs.gov

Homeland Security

Communications Sector Sector Risk Snapshot

Figure 1: U.S. Households with Computers, Telephone Subscriptions, and Internet Access, Selected Years, 1997-2010



*Note: 2001-2012 use 2000 Census-based weights and earlier years use 1990 Census-based weights
Source: National Telecommunications and Information Administration, February 2011

Types of Communications Infrastructure

- **Wireline Communications**: Consists primarily of the public switched telephone network (PSTN) and includes cable networks and enterprise networks. Wireline networks also are being redefined by next generation networks (NGNs), which are high-speed, converged circuit-switched and packet-switched networks capable of transporting and routing a multitude of services, including voice, data, video, and other multimedia, across various platforms. The wireline component also includes the Internet infrastructure and submarine cable infrastructure.
- **Wireless Communications:** Consists primarily of cellular telephone, paging, personal communications services, high-frequency radio, unlicensed wireless, and other commercial and private radio services, including numerous law enforcement, public safety, and land mobile radio systems.
- **Satellite Communications:** Satellite communications systems deliver data, voice, and video services. Networks may be private and independent of the terrestrial infrastructure or may share common facilities (e.g., a teleport) and be combined with terrestrial services to deliver information to the intended recipient(s). Important satellite network components include ground stations; telemetry, tracking, and command links (TT&Cs); very small aperture terminals (VSATs); and data links.
- **Cable:** Cable communications systems are wireline networks that offer analog and digital video programming services, digital telephone service, and high-speed Internet access service. Cable systems use a mixture of fiber and coaxial cable that provide two-way signal paths to the customer.
- **Broadcasting:** Broadcasting systems consist of free, over-the-air radio and television stations that offer analog and digital audio and video programming services and data services.

Communications Sector Overview

- **The Communications Sector is an integral component of the U.S. economy, underlying the operations of all businesses, public safety organizations, and government. Over the last 25 years, the Sector has evolved from predominantly a provider of voice services into a diverse, competitive, and interconnected industry, using terrestrial, satellite, and wireless transmission systems.**
- **The transmission of these services has become very interconnected; satellite, wireless, and wireline providers depend on each other to carry and terminate their traffic, and companies routinely share facilities and technology to ensure interoperability and efficiency.**
- **The private sector, as owners and operators of the majority of communications infrastructure, is the primary entity responsible for protecting Sector infrastructure and assets.**
- **Working with the Federal Government, the private sector is able to predict, anticipate, and respond to Sector outages and understand how they might affect the ability of the national leadership to communicate during times of crisis, impact the operations of other Sectors, and affect response and recovery efforts.**
- **The Communications Sector is closely linked to a number of other Sectors, including Energy, Information Technology, Financial Services, Emergency Services, and Postal and Shipping.**

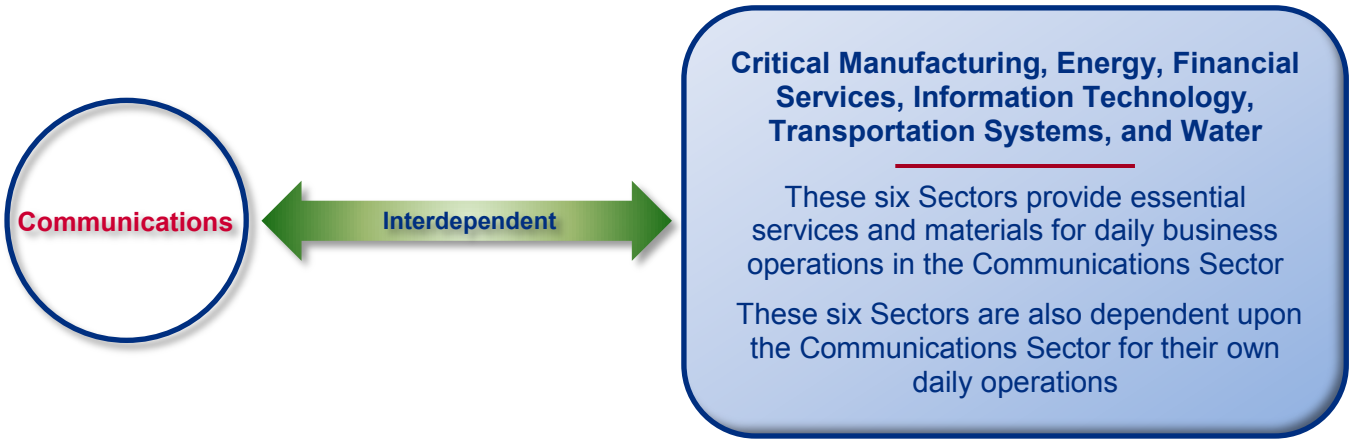
Threats and Hazards of Significant Concern

- **Single physical incidents**, such as nuclear detonations, major earthquakes, hurricanes, and space weather are likely to significantly disrupt the Sector over large regions. The Sector hardens systems and applies the principle of diversity (employing various primary and alternative routing and systems) and the principle of redundancy (using backup or multiple capabilities to sustain operations) to mitigate these and other threats (e.g., those that could cause potential damage to underground infrastructure from digging).
  - Space weather, such as severe solar geomagnetic storms, can cause high-power transformers to fail and electrical systems to possibly collapse. Because of the dependence of communications systems on electrical power, communications networks would soon fail in the event of a long-term, large-scale electrical network collapse. Solar weather can also directly degrade communications satellites and disrupt global positioning system (GPS) functionality (interfering with GPS satellites and their signals). Short-term loss or disruption of GPS will have minimal impacts on the underlying infrastructure, but medium- to long-term loss will degrade GPS-reliant services provided through the wireless, satellite, cable, and broadcast networks.
- **Cyber-disruptions** of communications systems present unique challenges due to global connectivity. The exploitation of vulnerabilities halfway around the world can begin affecting critical U.S. communications components in a matter of minutes.
- **Malicious actors** pose one of many human risks, which can impact data, networks, and components, as well as create financial losses for organizations.
  - The use of high-altitude electromagnetic pulse (EMP) weapons, source region EMP weapons, intentional electromagnetic interference devices, and high-energy radio frequency weapons could damage both electrical and communications systems.
  - Breached supply chain integrity could also result in disruption of service and network availability, loss of network control, loss of confidentiality and integrity of communications, unauthorized access, and disruption of emergency telecommunications, as well as fraud and theft of service.

For More Information

- Sector-Specific Agency: DHS, Office of Cybersecurity and Communications, www.dhs.gov/office-cybersecurity-and-communications
- DHS, *National Risk Profile,* OCIA@hq.dhs.gov
- DHS, www.dhs.gov/communications-sector

Figure 2: Common, First-order Interdependencies of the Communications Sector



May 2014

Homeland Security

Prepared by the DHS National Protection and Programs Directorate
Office of Cyber and Infrastructure Analysis (OCIA)
Questions or comments should be directed to OCIA@hq.dhs.gov

Homeland Security

Critical Manufacturing Sector
Sector Risk Snapshot

Figure 1: Manufacturing's Role in the U.S. Economy

* Exports data from 2010. R&D Data from 2009, the last available. All other data from 2011.
Source: U.S. Department of the Treasury

Several characteristics of today's manufacturing environment are common across each of the key functional areas within the Critical Manufacturing Sector. Examples include the following:

1. **Most manufacturing enterprises are integrated into complex, interdependent supply chains.** Few businesses operate independently. Nearly all manufacturers are part of a chain of suppliers, vendors, partners, integrators, contractors, and customers that link to other industries and businesses.
2. **Supply chains have been optimized for productivity and efficiency.** Competitive pressures cause businesses to optimize their manufacturing processes through highly coordinated business arrangements that enable manufacturers to maintain low inventories of raw materials and intermediate and end products.
3. **Manufacturers have become highly reliant on global information and communication systems.** Automation, control, information, processing, robotics, telecommunications, and the Internet have radically improved industrial productivity and have reshaped the operations and asset base of manufacturers.
4. **Globalization and outsourcing have linked U.S. manufacturers with foreign suppliers, vendors, and customers through highly interdependent supply networks.** Manufacturers have increasingly turned to foreign markets for raw materials, component manufacturing, equipment and machinery, labor, and customers as a way to reduce overall costs.
5. **Manufacturers rely heavily on energy sources for heat, power, and raw materials.** While all businesses are dependent on energy, manufacturers typically require large amounts of these resources, much of it in the form of hard-to-store electricity and natural gas.

Critical Manufacturing Sector Overview

- **The Critical Manufacturing Sector is crucial to the economic prosperity and continuity of the United States. Products designed, produced, and distributed by U.S. manufacturers make up 12 percent of the U.S. gross domestic product and directly employ nearly 12 million of the Nation's workforce.**
- **The Critical Manufacturing Sector identified the following industries to serve as the core of the Sector:**
  - **Primary Metal Manufacturing**
  - **Machinery Manufacturing**
  - **Electrical Equipment, Appliance, and Component Manufacturing**
  - **Transportation Equipment Manufacturing**
- **These key functional areas depend upon physical, cyber, and human elements to perform their missions:**
  - **Physical elements include the facilities supporting each functional area.**
  - **Human elements include the personnel associated with each function.**
  - **The cyber-elements include electronic systems for processing the information necessary for management and operation or for automatic control of physical processes.**
- **Each key functional area has unique markets, assets, business models, and competitive conditions that shape the critical manufacturing risk profile.**
- **Products made by these manufacturing industries are essential in varying capacities to many other critical infrastructure sectors.**

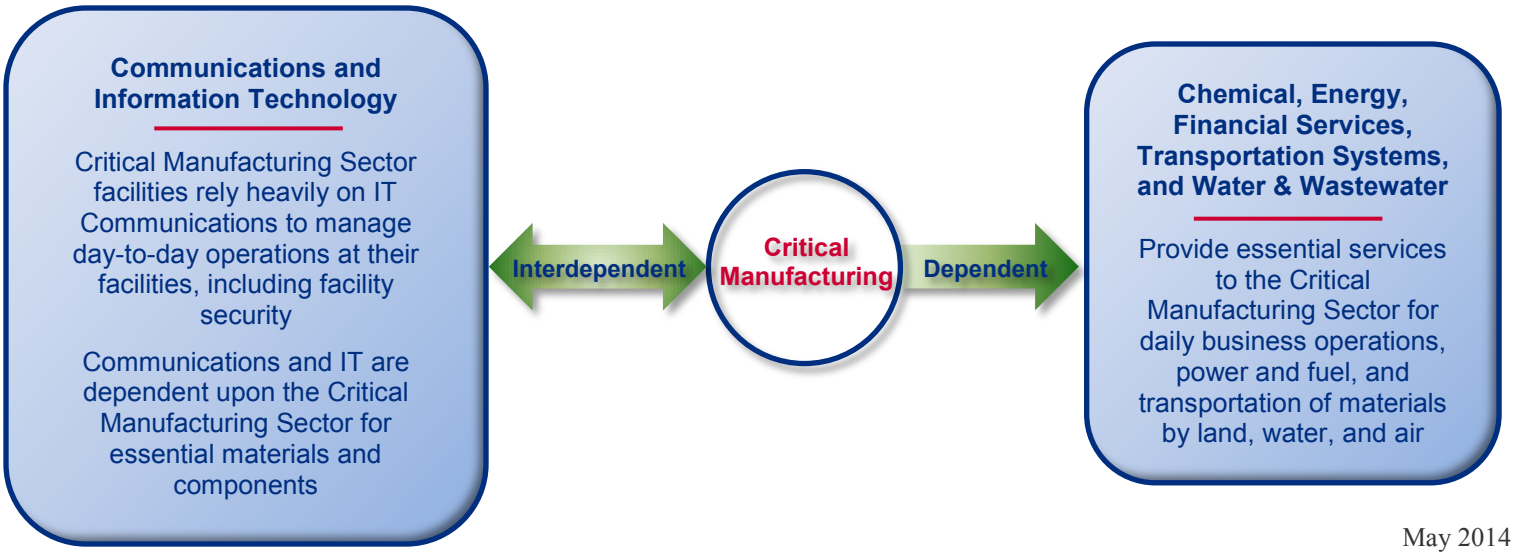
Threats and Hazards of Significant Concern

- **Supply Chain Vulnerability**
  - Supply chains at key inbound transportation nodes are of particular concern because incidents are likely at nodes, such as domestic ports. There is also a potential for large-scale consequences to the many industries that rely on the importation of materials and products.
  - Lean inventory and just-in-time practices, as well as greater distances from components or raw materials required for production to the delivery of finished products to markets, have made the Critical Manufacturing Sector more sensitive to transportation disruptions and fuel costs.
  - Supply chain systems are also more vulnerable because fewer basic metals and minerals are mined and processed in the United States, thereby increasing our dependence on foreign countries to provide these materials.
- **Cyberthreats**
  - Unauthorized on-site or remote intrusion into sector industrial control systems and supervisory control and data acquisition systems poses a growing threat and contributes to risk for the Critical Manufacturing Sector.
  - Supply chain systems are more vulnerable because of increased reliance on advanced information technology (IT) systems. Critical infrastructure owners and operators are also slow to adopt security and risk management measures for systems. Nation-states and other actors could potentially defeat competition and/or obtain competitive secrets through cyberintrusion.
- **Insider Threat**
  - The sector's systems are complex and increasingly dependent on information technology, making the sector highly susceptible to exploitation by current and former industry employees and contractors with malicious intent and unique knowledge of, and access to, these systems.
  - Threats posed by malicious insiders may include sabotage, theft or diversion, cyberattacks, or terrorism against critical manufacturing facilities.

For More Information

- Sector-Specific Agency: DHS, Office of Infrastructure Protection, www.dhs.gov/about-office-infrastructure-protection
- DHS, Sector Specific Profile: www.dhs.gov/critical-manufacturing-sector-critical-infrastructure
- DHS, *National Risk Profile*, OCIA@hq.dhs.gov

Figure 2: Common, First-order Dependencies and Interdependencies of the Critical Manufacturing Sector



May 2014

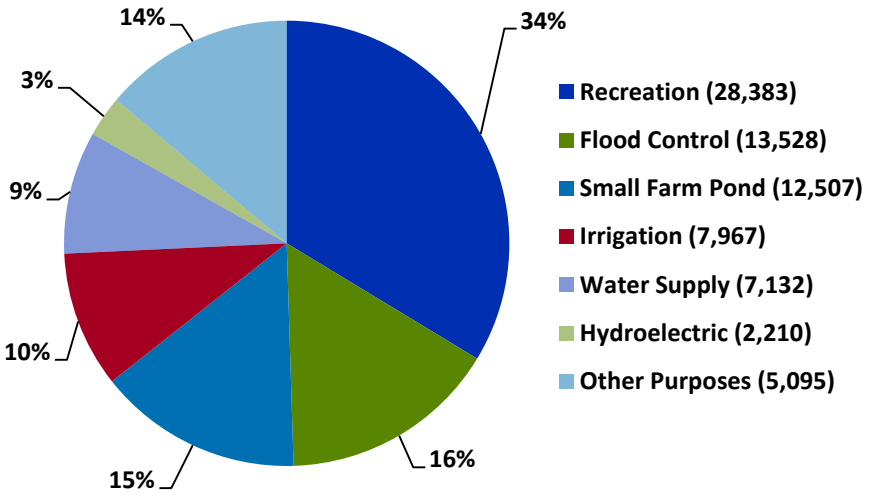
Homeland Security

Prepared by the DHS National Protection and Programs Directorate
Office of Cyber and Infrastructure Analysis (OCIA)
Questions or comments should be directed to OCIA@hq.dhs.gov

Homeland Security

Dams Sector Sector Risk Snapshot

Figure 1: Primary Purpose or Benefit of U.S. Dams



Dams Sector assets are vital components of the Nation's infrastructure. Some examples of the benefits derived from sector assets are:

Water Storage and Irrigation: Dams create reservoirs that supply water for a multitude of industrial, municipal, agricultural, and recreational uses throughout the United States.

Electricity Generation: Dams in the United States produce more than 270,000 gigawatt-hours of the Nation's electricity, representing 70 percent of the Nation's renewable energy generation, and over 6 percent of U.S. electricity generation overall.

"Black Start" Capabilities: There are 4,316 megawatts of "incremental" hydropower available at sites with existing hydroelectric facilities. Incremental is defined as capacity additions or improved efficiency at existing hydro projects.

Recreation: Dams and other sector assets provide prime recreational facilities throughout the United States.

Navigation: The U.S. waterway system, which includes 236 lock chambers at 192 lock sites owned and/or operated by the U.S. Army Corps of Engineers (USACE).

Flood Risk Reduction: Many dams and levees function as flood control projects, thereby reducing the potential human health and economic impacts of flooding.

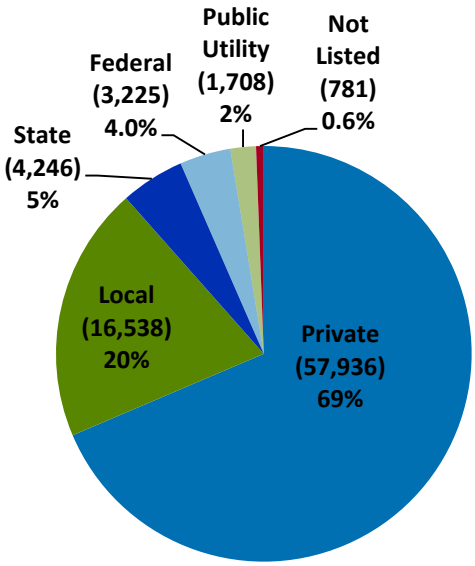
Sediment Control: Some dams enhance environmental protection by controlling detrimental sedimentation.

Impoundment of Mine Tailings and Industrial Waste Materials: More than 1,500 mine tailings and industrial waste impoundments controlled by dams in the Nation facilitate mining and processing of coal and other vital minerals.

Dams Sector Overview

- **The Dams Sector comprises assets that include dam projects, hydropower generation facilities, navigation locks, levees, dikes, hurricane barriers, mine tailings, industrial waste impoundments, and other similar water retention and water control facilities.**
- **The Dams Sector is a vital and beneficial part of the Nation's infrastructure. It continuously provides a wide range of economic, environmental, and social benefits, including hydroelectric power, river navigation, water supply, wildlife habitat, waste management, flood control, and recreation.**
- **There are more than 84,000 dams in the United States; approximately 69 percent are privately owned, and more than 85 percent are regulated by State dam safety offices.**

Figure 2: Dam Ownership in the U.S.



Source Figures 1-2: DHS, Dams Sector-Specific Plan, *2010, www.dhs.gov/dams-sector.*

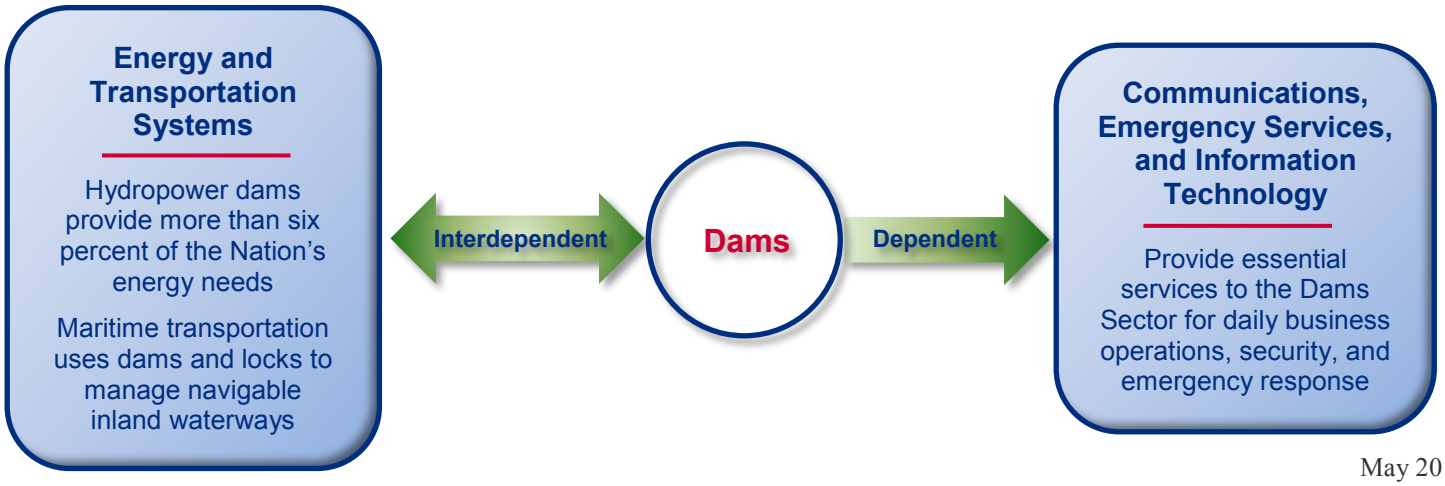
Threats and Hazards of Significant Concern

- **Natural Hazards**
  - Extreme flooding and severe storm surges can overwhelm the flood storage capacity of reservoirs and levee systems and lead to breaching or overtopping.
  - The consequences of extreme levee failure were seen in the aftermath of Hurricanes Katrina and Rita in 2005, which resulted in the deaths of more than 1,800 people and more than $200 billion in economic damages.
  - Earthquake ground motion may also lead to severe damage or failure, as evidenced by the failure of Fujinuma Dam in Japan following the Tōhoku earthquake in March 2011.
- **Malicious Actors**
  - With the necessary capabilities and resources, adversaries could potentially achieve catastrophic failure and severely disrupt missions through the use of improvised explosive devices (IEDs), increasing risk for the Sector.
  - Dams Sector assets have experienced at least 20 kinetic attacks worldwide over the last decade, and adversaries could exploit the inherent vulnerabilities of these public facilities (Source: National Consortium for the Study of Terrorism and Responses to Terrorism, Global Terrorism Database, 2011).
  - Adversaries could bypass land-based security measures with water-borne IEDs and strike dams, locks, or levees. Vehicle-borne IEDs (VBIEDs) could also reach the crest of dams or levees, particularly those with roads providing vehicular access. An assault team could overpower security forces, seize a facility's control room, and detonate IEDs, as occurred in a July 2010 attack against a Russian hydropower station.
  - The increasing use of standardized industrial control systems (ICS) technology increases the sector's potential vulnerability to direct cyberattacks and intrusions, which are a constant potential threat across the critical infrastructure community.
- **Aging Infrastructure**
  - Some dams, inland waterways, and levees are in increasingly poor condition as a result of aging, deterioration, and maintenance backlogs. This increases the risk to the Dams Sector, as its infrastructure continues to age.
  - The average age of the 84,000 dams in the country is 52 years old. The number of deficient dams is estimated at more than 4,000, which includes 2,000 deficient high-hazards dams. In addition, 91 percent of U.S. levees are not in acceptable condition (Source: American Society of Civil Engineers, *Infrastructure Report Card,* 2013).

For More Information

- Sector-Specific Agency: DHS, Office of Infrastructure Protection, www.dhs.gov/dams-sector
- DHS, *National Risk Profile*, OCIA@hq.dhs.gov
- DHS, *Dams Sector: Roadmap to Secure Control Systems,*2010
- USACE, National Inventory of Dams, http://nid.usace.army.mil

Figure 3: Common, First-order Dependencies and Interdependencies of the Dams Sector



May 2014

Homeland Security

Prepared by the DHS National Protection and Programs Directorate
Office of Cyber and Infrastructure Analysis (OCIA)
Questions or comments should be directed to OCIA@hq.dhs.gov

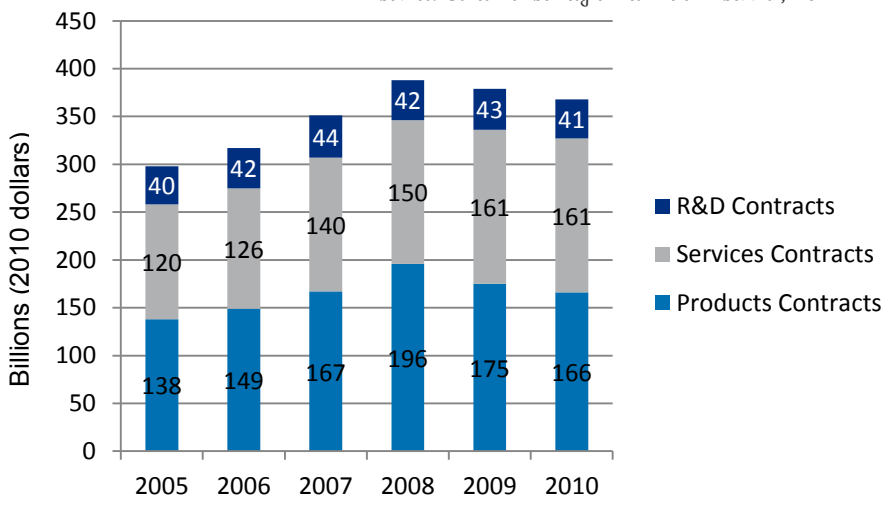
Homeland Security

Defense Industrial Base Sector
Sector Risk Snapshot

The Defense enterprise is the largest and most complex organization in the world. In addition to managing roughly three million employees, a budget of more than $600 billion, operating almost 5,000 locations, and providing healthcare for 9.6 million military members, retirees, and their families, the DOD also executes a multibillion dollar global supply chain that manages an inventory of five million line items.

Figure 1: U.S. Department of Defense Contract Spending and the Supporting Industrial Base

Source: Center for Strategic International Studies, 2011



Defense Industrial Base Sector Goals

Sector Risk Management: Use an all-hazards approach to manage the risk-related dependency on critical DIB assets.

Collaboration, Information Sharing, and Training: Improve collaboration within a shared knowledge environment in the context of statutory, regulatory, proprietary, and other pertinent information-sharing constraints and guidance.

Personnel Security: Mitigate the risk created by personnel with unescorted physical or logical access to critical DIB assets in conformance with pertinent industry best practices, including regulatory and statutory requirements.

Physical Security: Manage the risk created by threats to and vulnerabilities of critical DIB physical assets.

Information Security [Cybersecurity/Information Assurances (CS/IA)]: Manage risk to information that identifies or describes characteristics or capabilities of DIB critical infrastructure and key resources, or that by nature would represent a high risk/high impact to critical infrastructure, resources, or DIB assets.

Defense Industrial Base Sector Overview

- **The Defense Industrial Base (DIB) is the worldwide industrial complex that enables research and development, as well as design, production, delivery, and maintenance of military weapons systems, subsystems, and components or parts to meet U.S. military requirements.**
- **Only a small fraction of DIB facilities are DOD-owned. The government component of DIB consists of certain laboratories, special-purpose manufacturing facilities, capabilities for production of uniquely military material such as arsenals and ammunition plants, and other services.**
- **The private sector component of the DIB consists of hundreds of thousands of independent, competing domestic and foreign companies and supply chains, delivering a vast array of products and services to DOD. DIB defense-related products and services equip, inform, mobilize, deploy, and sustain U.S. military and allied military forces worldwide. The DIB companies also deliver national security products and services to other Federal agencies.**
- **DIB does not include commercial infrastructure, such as communications, transportation, power, or other utilities, which serve as critical dependencies of the DIB Sector.**
- **The DIB Sector vision is to collaboratively eliminate or mitigate unacceptable levels of risk to physical, human, and cyber infrastructures, thus ensuring that DOD continues to fulfill its mission, and that DIB activities supporting national security objectives, public health and safety, and public confidence are effective.**

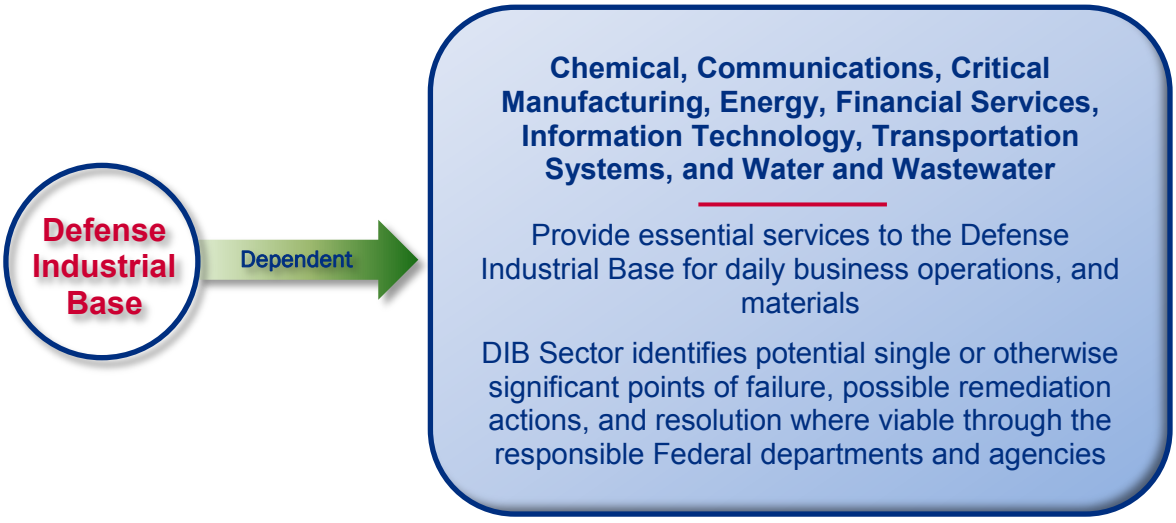
Threats and Hazards of Significant Concern

- **Cyberthreats**
  - The DIB Sector has become heavily dependent on cyber infrastructure, operating within an increasingly information-driven environment.
  - Cyber infrastructure is vulnerable to denial-of-service attacks and malicious modification of information, along with more mundane yet disruptive events, such as system malfunctions, power outages, and human error.
  - These vulnerabilities, combined with the increasing frequency and severity of cyberattacks across the critical infrastructure community, contribute greatly to the risk to the Sector. Foreign entities and non-state actors are also expected to continue seeking to acquire access to sensitive and classified DIB Sector information and technologies by expanding their cyber-collection activities [DOD, *Strategy for Operating in Cyberspace*, July 2011].
- **Loss of Supply Chain Integrity**
  - Due in part to a lack of traceability from foreign producers, potential loss of supply chain integrity (including related manufacturing and material availability) increases risk for the Sector.
  - This is highlighted by the ongoing infiltration of counterfeit electronics into the Sector. Lack of supply chain integrity could lead to the introduction of counterfeit materials, components, and technology into military equipment, which could, in turn, lead to equipment failures and increase risk in the field.

For More Information

- Sector-Specific Agency: Department of Defense, www.defense.gov
- DHS, *National Risk Profile,* OCIA@hq.dhs.gov
- DHS, www.dhs.gov/defense-industrial-base-sector
- Defense Industrial Base, *Sector Specific Plan (SSP),* 2010, www.dhs.gov/xlibrary/assets/nipp-ssp-defense-industrial-base-2010.pdf
- DOD, Defense Critical Infrastructure Program (DCIP), http://dcip.dtic.mil/index.html

Figure 2: Common, First-order Dependencies of the Defense Industrial Base Sector



May 2014

Homeland Security

Prepared by the DHS National Protection and Programs Directorate
Office of Cyber and Infrastructure Analysis (OCIA)
Questions or comments should be directed to OCIA@hq.dhs.gov

Homeland Security

Energy Sector
Electricity Subsector
Sector Risk Snapshot

Figure 1: U.S. Electric Transmission Grid

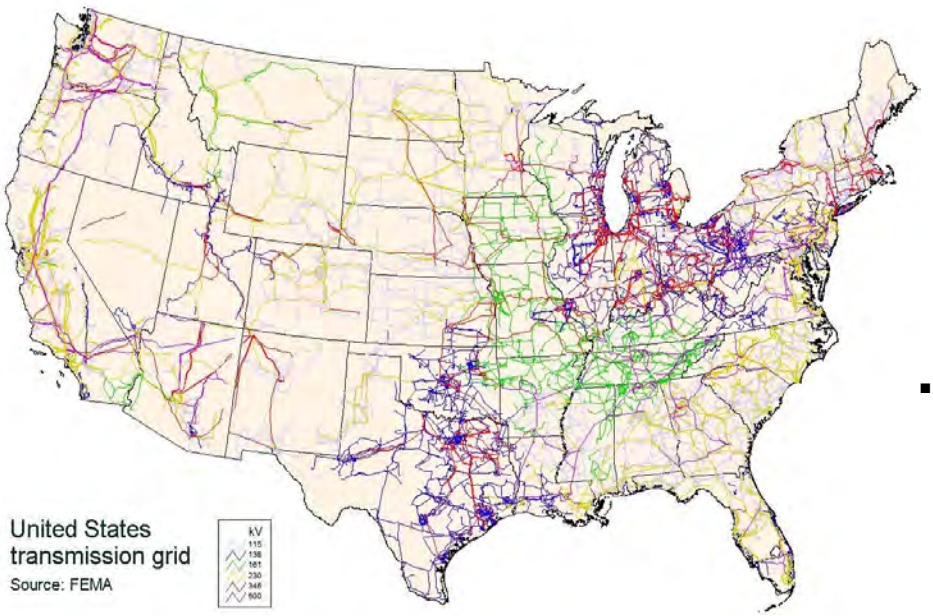
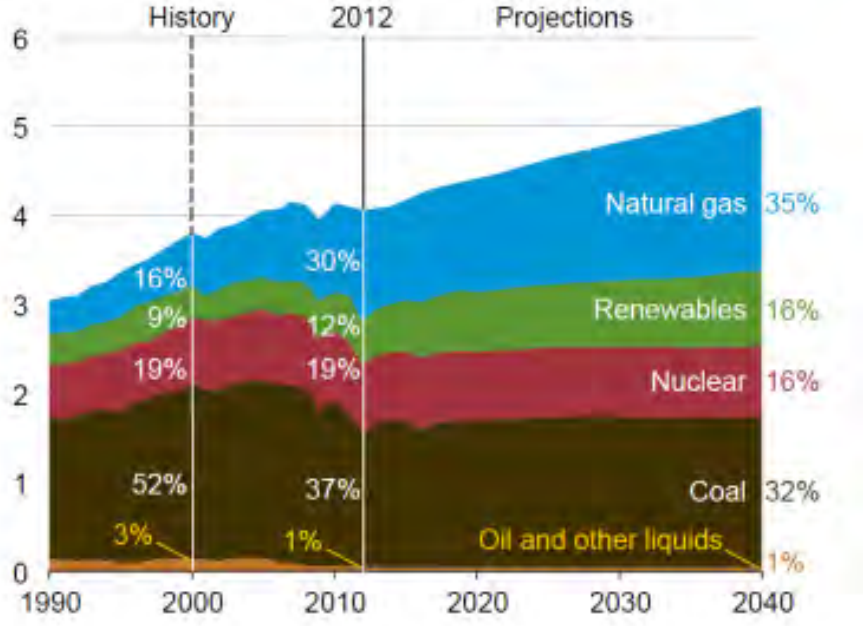


Figure 2: U.S. Electricity Generation by Fuel, 1990-2040 (trillion kilowatt hours)



Source: EIA, *Annual Energy Outlook Early Release Overview*, December 16, 2013, www.eia.gov/forecasts/aeo/er/index.cfm.

Electricity Subsector Overview

- **U.S. energy infrastructure fuels the economy of the 21st century. Without a stable energy supply, health and welfare are threatened, and the U.S. economy cannot function. More than 80 percent of the country's energy infrastructure is owned by the private sector, supplying fuels to the transportation industry, electricity to households and businesses, and other sources of energy that are integral to the Nation's growth and production.**
- **The Energy Sector is divided into three interrelated segments: electricity, petroleum, and natural gas. According to the Energy Information Administration (EIA), in 2011 there were 18,530 power generation facilities with a combined nameplate capacity of 1,153 gigawatts.**
- **More than 98 percent of electricity is generated domestically, although some significant regional differences exist and some of the fuels used to generate electricity are imported.**
- **The primary fuel for electric power generation is coal (37 percent), followed by natural gas (30 percent), nuclear (19 percent), renewable energy sources such as hydro, solar, or wind (12 percent), and other (1 percent). (Source: EIA, 2013)**
- **The electricity infrastructure is highly automated and controlled by utilities and regional grid operators, using sophisticated energy management systems, such as supervisory control and data acquisition systems (SCADA) or distributed control systems, to keep the system in balance.**
- **The reliance of virtually all industries and modes on electric power means that all Sectors have some dependence on the Energy Sector.**

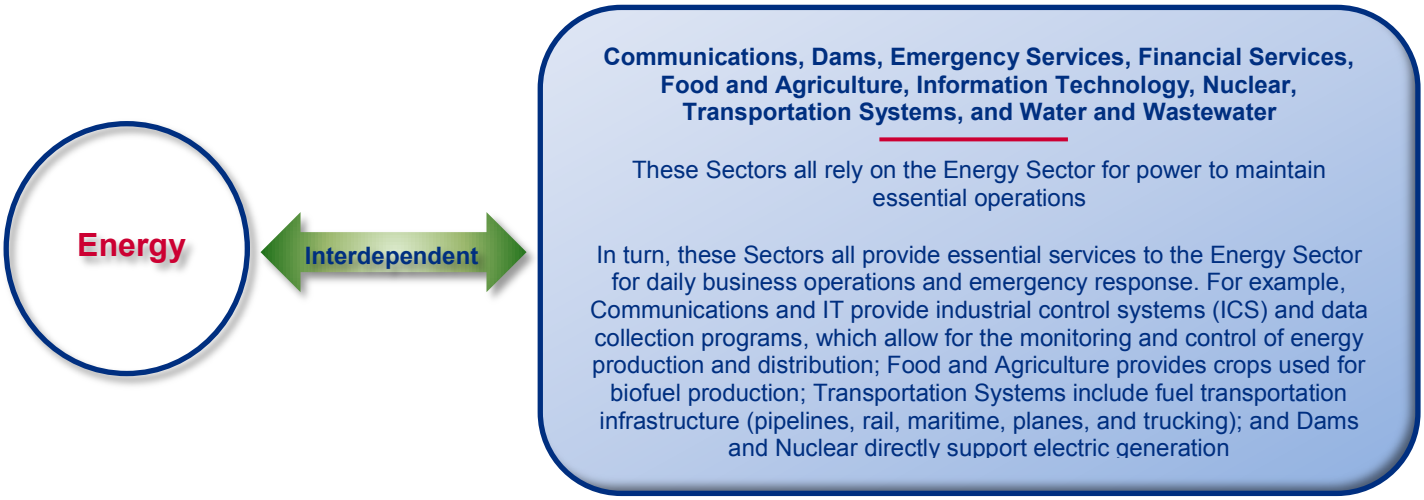
Threats and Hazards of Significant Concern

- **Cyberthreats**
  - Electricity infrastructure is highly automated and controlled by utilities and regional grid operators that rely on sophisticated energy management systems. For example, assets may be vulnerable if the Electricity Subsector's control system networks are connected to the corporate business network, which, in turn, is connected to the Internet. These connections increase the network's vulnerability to direct cyberattacks that could potentially disrupt power and increase risk to the Sector.
  - Insider threats, such as cyber-hacks initiated by current or former employees, increase the risk to the Electricity Subsector. These vulnerabilities are addressed to varying degrees across the Electricity Subsector, through a mix of voluntary and mandatory security standards that apply to electricity grid owners and operators.
- **Physical Attacks**
  - Physical attacks are a risk for the Sector's continued reliable operations. Coordinated physical attacks in the United States could produce wide-ranging impacts to both infrastructure and the reliability of the system.
  - Worldwide, terrorists have executed 2,523 attacks against energy infrastructure since 2004, leaving 1,852 dead and 4,653 wounded (National Counterterrorism Center, *Worldwide Incident Tracking System*, 2011). Moreover, successful strikes against individual Sector assets could lead to regional or nationwide impacts.
- **Natural Disasters**
  - Natural events, such as hurricanes, earthquakes, winter storms, wildfires, and solar flares, are a key risk of the Electricity Subsector, as these events occur regularly and have the capacity to cause extensive and widespread damage, impacting an area from days to weeks.
  - As all other Sectors have some degree of dependency upon the Electricity Subsector for normal operations, electric power restoration is a top priority following a natural disaster.

For More Information

- Sector-Specific Agency: Department of Energy, http://energy.gov/
- EIA, www.eia.gov
- DHS, *National Risk Profile,* OCIA@hq.dhs.gov
- DHS, www.dhs.gov/energy-sector

Figure 3: Common, First-order Interdependencies of the Energy Sector



May 2014

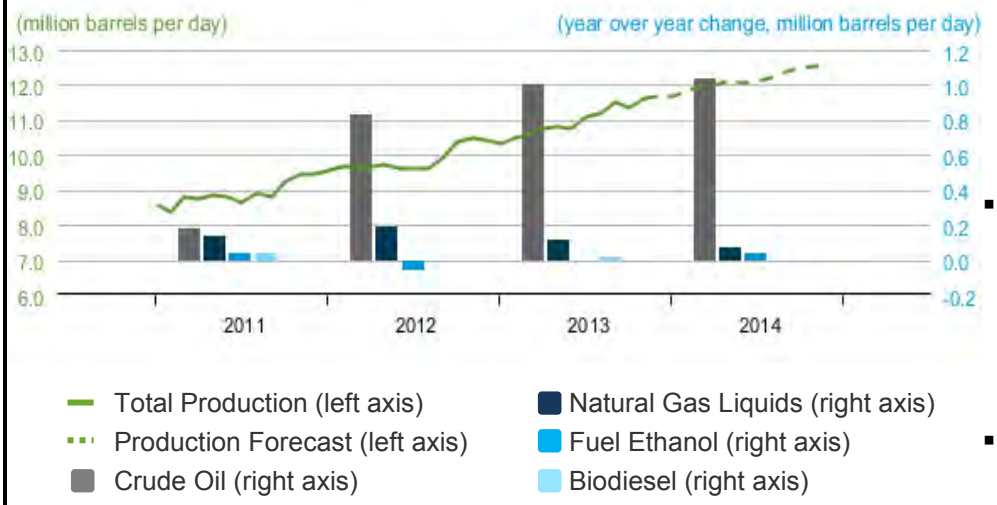
Homeland Security

Prepared by the DHS National Protection and Programs Directorate
Office of Cyber and Infrastructure Analysis (OCIA)
Questions or comments should be directed to OCIA@hq.dhs.gov

Homeland Security

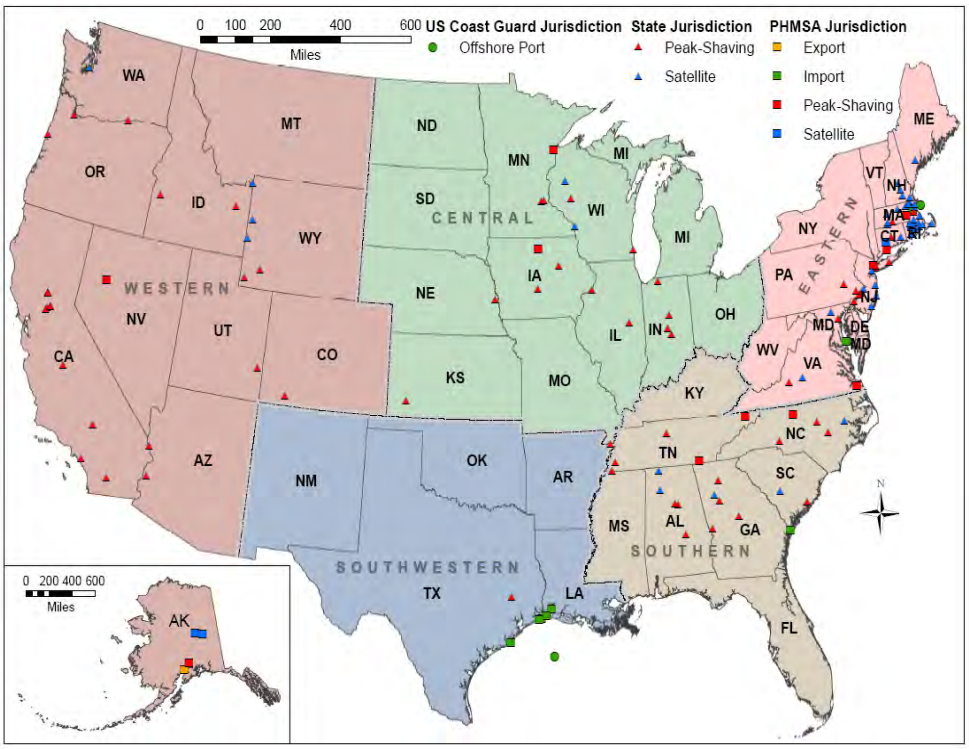
Energy Sector
Oil and Natural Gas Subsector
Sector Risk Snapshot

Figure 1: U.S. Crude Oil and Liquid Fuels Production



Source: U.S. Energy Information Administration, Short-Term Energy Outlook, 2013

Figure 2: U.S. Liquefied Natural Gas (LNG) Facilities Connected to Natural Gas Pipeline Systems



Source: U.S. Department of Transportation

Oil and Natural Gas Subsector Overview

- The petroleum section entails the exploration, production, storage, transport, and refinement of crude oil. The crude oil is refined into petroleum products that are then stored and distributed to key economic sectors throughout the United States.
- Key petroleum products include motor gasoline, jet fuel, distillate fuel oil, residual fuel oil, and liquefied petroleum gases. In the United States, there are more than 536,000 crude oil-producing wells, 30,000 miles of gathering pipeline, and 55,000 miles of crude oil pipeline.
- There are 150 operable petroleum refineries, 64,000 miles of product pipeline, and over 1,400 petroleum terminals.
- Natural gas is produced, piped, stored, and distributed in the United States. Imports of liquefied natural gas (LNG) fell 23 percent in 2012 due to unprecedented levels of domestic natural gas production, and companies are now applying to the Department of Energy to export domestic LNG to foreign countries. There are more than 514,000 gas production and condensate wells and 19,000 miles of gathering pipeline in the United States. There are almost 304,000 miles of interstate and intrastate pipeline for the transmission of natural gas.
- Natural gas is distributed to homes and businesses over 1,200,000 miles of distribution pipelines. The heavy reliance on pipelines to distribute products across the Nation highlights the interdependencies between the Energy and Transportation Systems Sectors.
- The reliance of virtually all industries and modes on fuels means that all Sectors have some dependence on the Energy Sector.

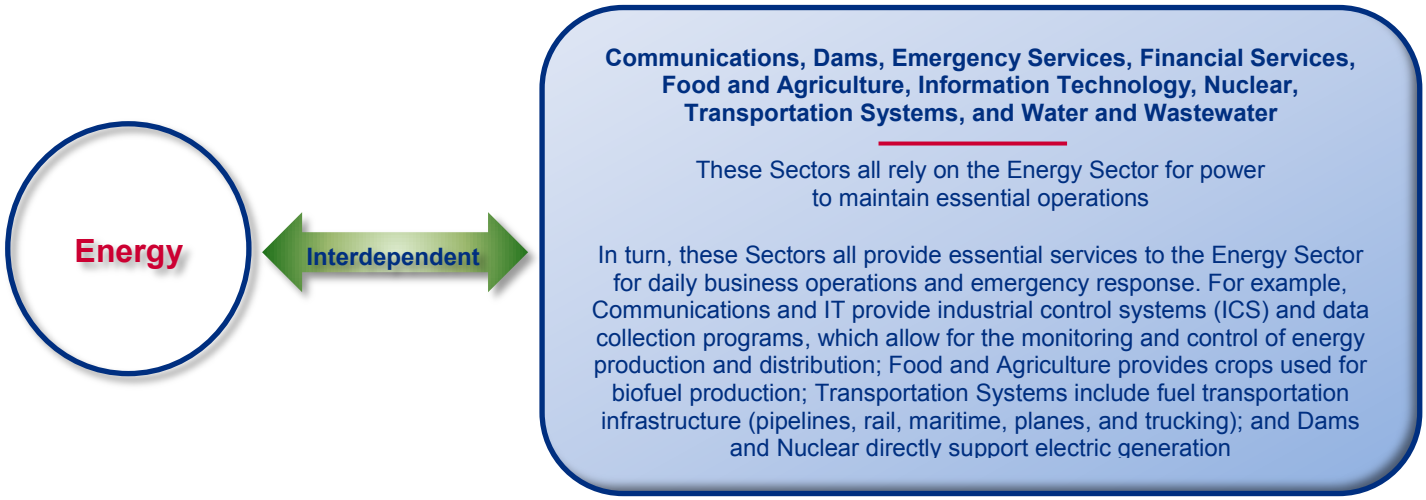
Threats and Hazards of Significant Concern

- **Cyberthreats**
  - Oil and natural gas infrastructure is highly automated and controlled by pipeline operators, terminal owners, and natural gas utilities that rely on sophisticated energy management systems. Assets may be vulnerable if these industrial control systems are connected to the Internet, either directly or indirectly. For example, control system networks may be connected to the corporate business network, which, in turn, is connected to the Internet. These connections increase the network's vulnerability to direct cyberattacks that could potentially disrupt movement and increase risk to the Sector.
  - Insider cyberthreats, such as those initiated by current or former employees, create risk to the Oil and Natural Gas Subsector. Cyber-actors can target industrial control systems (ICS) and gain control of a process within a refinery, pipeline, or terminal. A cyber-actor could manipulate the production, storage, and transportation aspects of oil and natural gas. These vulnerabilities are addressed to varying degrees across the Oil and Natural Gas Subsector, through a mix of voluntary and mandatory security standards that apply to owners and operators.
- **Physical Attacks**
  - Physical attacks are a risk for the Sector's continued reliable operation. Coordinated physical attacks in the United States could produce wide-ranging impacts to both infrastructure and the reliability of the system.
  - Worldwide, terrorists have executed 2,523 attacks against energy infrastructure since 2004, leaving 1,852 dead and 4,653 wounded (National Counterterrorism Center, *Worldwide Incident Tracking System*, 2011). Successful strikes against individual Sector assets could lead to cascading regional or nationwide impacts.
- **Natural Disasters**
  - Many natural disasters can affect the Oil and Natural Gas Subsector. Hurricanes are the most frequent disruptive natural hazard for the Subsector, often causing the preemptive shutdown of facilities in an area, even if the facilities themselves are not directly affected by the storm. Hurricanes Ike and Gustav impacted almost 65 million barrels of crude oil production and 400 billion cubic feet of the natural gas supply (Energy Information Administration, *2010 Outlook for Hurricane-Related Production Outages in the Gulf of Mexico*, 2010).

For More Information

- Sector-Specific Agency: Department of Energy, http://energy.gov/
- DHS, *National Risk Profile,* OCIA@hq.dhs.gov
- DHS, www.dhs.gov/energy-sector
- U.S. Department of Pipeline and Hazardous Materials Safety Administration (PHMSA), www.phmsa.dot.gov

Figure 3: Common, First-order Interdependencies of the Energy Sector



May 2014

Homeland Security

Prepared by the DHS National Protection and Programs Directorate
Office of Cyber and Infrastructure Analysis (OCIA)
Questions or comments should be directed to OCIA@hq.dhs.gov

Homeland Security

Emergency Services Sector Sector Risk Snapshot

Function/Discipline	Roles and Responsibilities
Law Enforcement	Maintaining law and order and protecting the public from harm. Law enforcement activities may include investigation, prevention, response, court security, and detention, as well as other associated capabilities and duties.
Fire and Emergency Services	Prevention and minimizing loss of life and property during incidents resulting from fire, medical emergencies, and other all-hazards events.
Emergency Medical Services	Providing emergency medical assessment and treatment at the scene of an incident, during an infectious disease outbreak, or during transport and delivery of injured or ill-individuals to a treatment facility as part of an organized EMS system.
Emergency Management	Leading efforts to mitigate, prepare for, respond to, and recover from all types of multijurisdictional incidents.
Public Works	Providing essential emergency functions, such as assessing damage to buildings, roads, and bridges; clearing, removing, and disposing of debris; restoring utility services; and managing emergency traffic.

Emergency Services Infrastructure

- Large, geographically distributed base of facilities, equipment, and highly skilled personnel who provide services in both paid and volunteer capacities.
- Largely organized at the State, local, tribal, and territorial levels of government, corresponding to the scales on which emergencies generally occur. The complex and dispersed nature of the Sector makes it difficult to disable the entire system; it also presents challenges in coordinating emergency responses across disciplines, regions, and levels of government.
- Relies heavily on complex communication and information technology systems to enable robust communications and appropriate coordination and management of diverse elements during emergency situations.
- Uses specialized transportation vehicles and secure transportation routes to facilitate Sector operations because personnel, equipment, aid, and victims must be moved to and from scenes of emergencies.
- The Sector focuses primarily on the protection of other sectors and people, rather than protecting the Sector itself, which presents unique challenges in addressing the protection of Emergency Services as a critical infrastructure sector.
- ESS involves primarily the public sector, but also includes private sector holdings, such as industrial fire departments, sworn private security officers, and private EMS providers.

Emergency Services Sector Overview

- **The Emergency Services Sector (ESS) comprises five disciplines: Law Enforcement, Fire and Rescue Services, Emergency Medical Services (EMS), Emergency Management, and Public Works.**
- **In addition, there are specialized capabilities: Explosive Ordnance Disposal, Hazardous Materials Response, Special Weapons and Tactics and Tactical Operations, Search and Rescue, Aviation Units, and Public Safety Answering Points.**
- **Through partnerships with public and private sector entities, this Sector's mission is to save lives, protect property and the environment, assist communities impacted by disasters (natural or manmade), and aid recovery from emergency situations.**
- **ESS assets, systems, networks, and functions are critical to maintain, protect, and preserve the Nation's safety and health in case of naturally occurring or manmade threats and hazards. By protecting these elements, the Sector is better able to support all critical infrastructure, essential governmental missions, and public services.**
- **The Sector has dependencies and interdependencies with multiple critical infrastructure sectors and the National Response Framework's Emergency Support Functions that support both ESS operations and protection of ESS assets.**

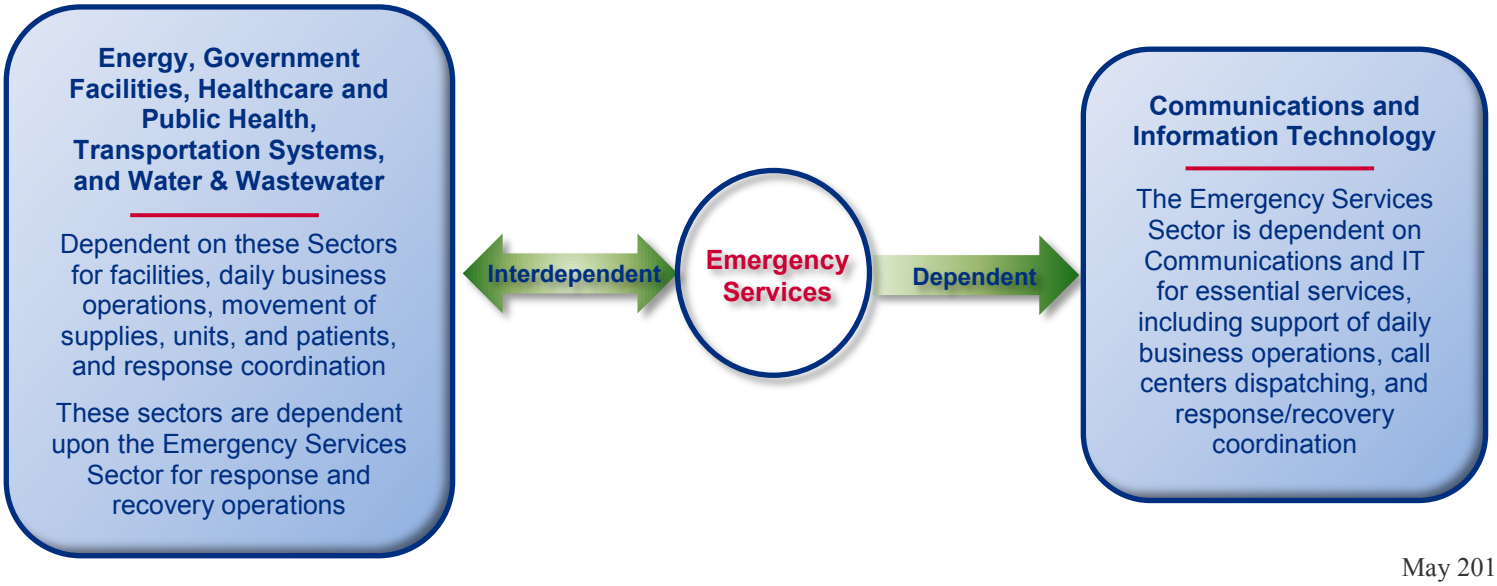
Threats and Hazards of Significant Concern

- **Communications Vulnerabilities**
  - Communication channels and equipment standards have improved dramatically in the last several years. However, many jurisdictions still struggle to use standardized emergency call codes and police radio codes, have difficulty obtaining bandwidth to transmit communications, lack interoperable communications equipment, and do not share frequencies among the various member organizations of the Sector (e.g., police and fire). All of these contribute to ongoing risk for the Sector.
- **Cyberthreats**
  - The dependence of the ESS on information technology also contributes to risk. For example, cyberdisruption of communications systems, computer networks in service vehicles, or GPS during an emergency operation could dramatically disrupt or delay the initial response to an event.
- **Malicious Actors**
  - Contribute significant risk to the Sector. Fire, police, hazardous materials, and other emergency service units respond to criminal threats, violent extremists, suspected terrorist events (e.g., mailed letters and packages containing white powders that could be anthrax), and the aftermath of terrorist attacks (e.g., the bombing of the Oklahoma City Murrah Federal Building, the events of September 11, 2001, and the anthrax events of 2001).
  - As a result, emergency services personnel are exposed to substances of unknown composition, for which their personal protective equipment may not provide adequate protection and from which there may be long-term health implications. Adversaries may also target persons in positions of authority, as well as institutions that are symbolic of a functioning society. ESS representatives may be attacked with improvised explosive devices or targeted by active shooters for these same reasons.

For More Information

- Sector-Specific Agency: DHS, Office of Infrastructure Protection, www.dhs.gov/about-office-infrastructure-protection
- DHS, *National Risk Profile,* OCIA@hq.dhs.gov
- DHS, www.dhs.gov/emergency-services-sector

Figure 1: Common, First-order Dependencies and Interdependencies of the Emergency Services Sector



May 2014

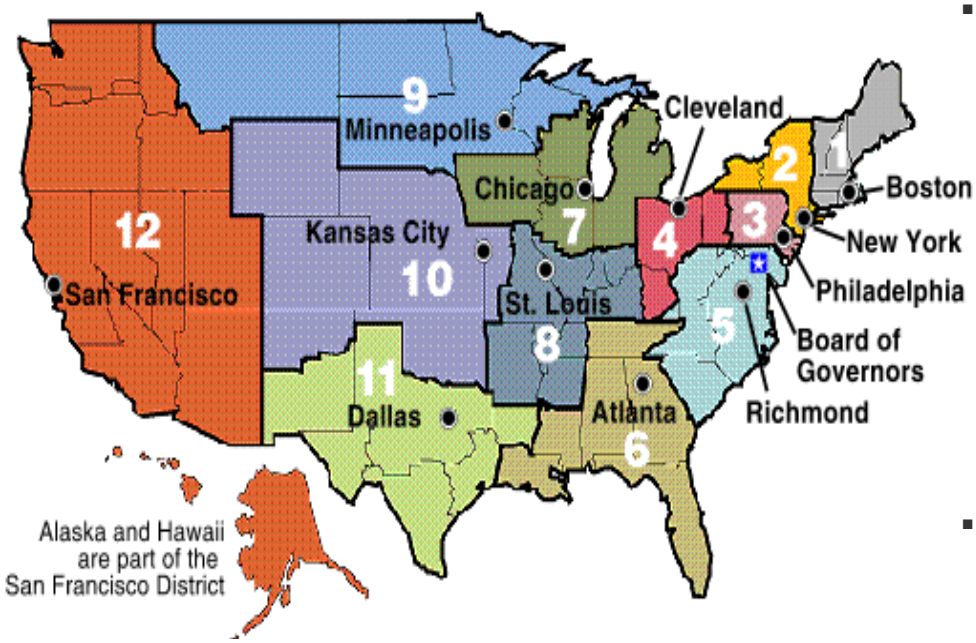
Homeland Security

Prepared by the DHS National Protection and Programs Directorate
Office of Cyber and Infrastructure Analysis (OCIA)
Questions or comments should be directed to OCIA@hq.dhs.gov

Homeland Security

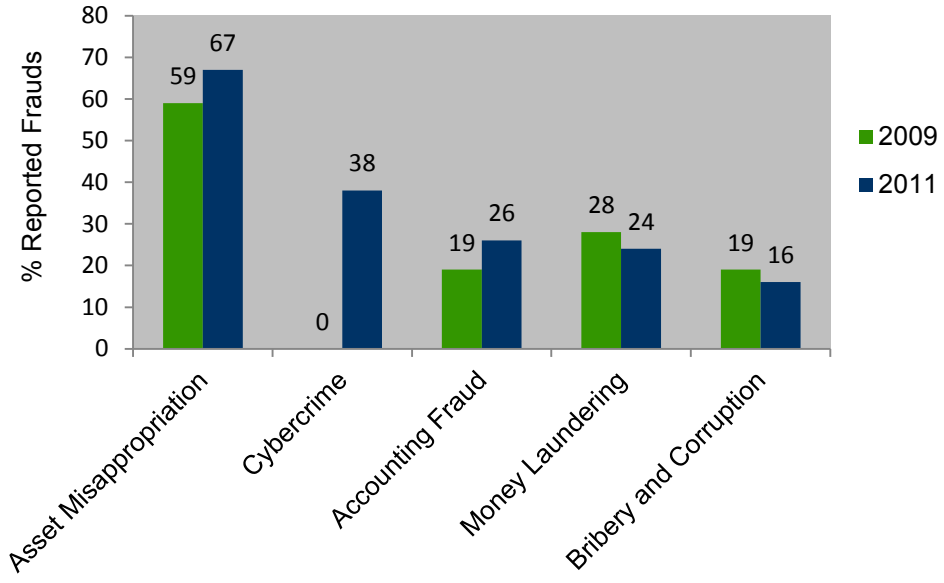
Financial Services Sector Sector Risk Snapshot

Figure 1: U.S. Federal Reserve Bank Locations and Districts



Source: The Federal Reserve Board, www.federalreserve.gov/otherfrb.htm

Figure 2: Top 5 Types of Economic Crimes Experienced by the Financial Services Sector, as Reported in a PwC 2011 Global Survey



Source: PricewaterhouseCoopers, LLP, *Fighting Economic Crime in the Financial Services Sector,* 2012, www.pwc.com/en_GX/gx/economic-crime-survey/pdf/fighting-economic-crime-in-the-financial-services-sector.pdf

Financial Services Sector Overview

- **The Financial Services Sector represents a vital component of the Nation's critical infrastructure. As the Sector-Specific Agency, the Department of the Treasury works with all relevant Federal Departments and agencies; State, local, and tribal governments; and the private sector to promote efforts to improve the Sector's ability to prepare for, respond to, prevent, and mitigate manmade threats, natural disasters, and other intentional or unintentional risks.**
- **Financial institutions provide a broad array of products from the largest institutions to the smallest community banks and credit unions. These products allow customers to do the following:**
  - **— Deposit funds and make payments to other parties;**
  - **— Provide credit and liquidity to customers;**
  - **— Invest funds for both long and short periods; and**
  - **— Transfer financial risks between customers.**
- **Financial institutions are organized and regulated, based on services provided by institutions. Within the sector, there are more than 18,800 federally insured depository institutions; thousands of providers of various investment products, including roughly 18,440 broker-dealer, investment adviser, and investment company complexes; providers of risk transfer products, including 7,948 domestic U.S. insurers; and thousands of other credit and financing organizations.**

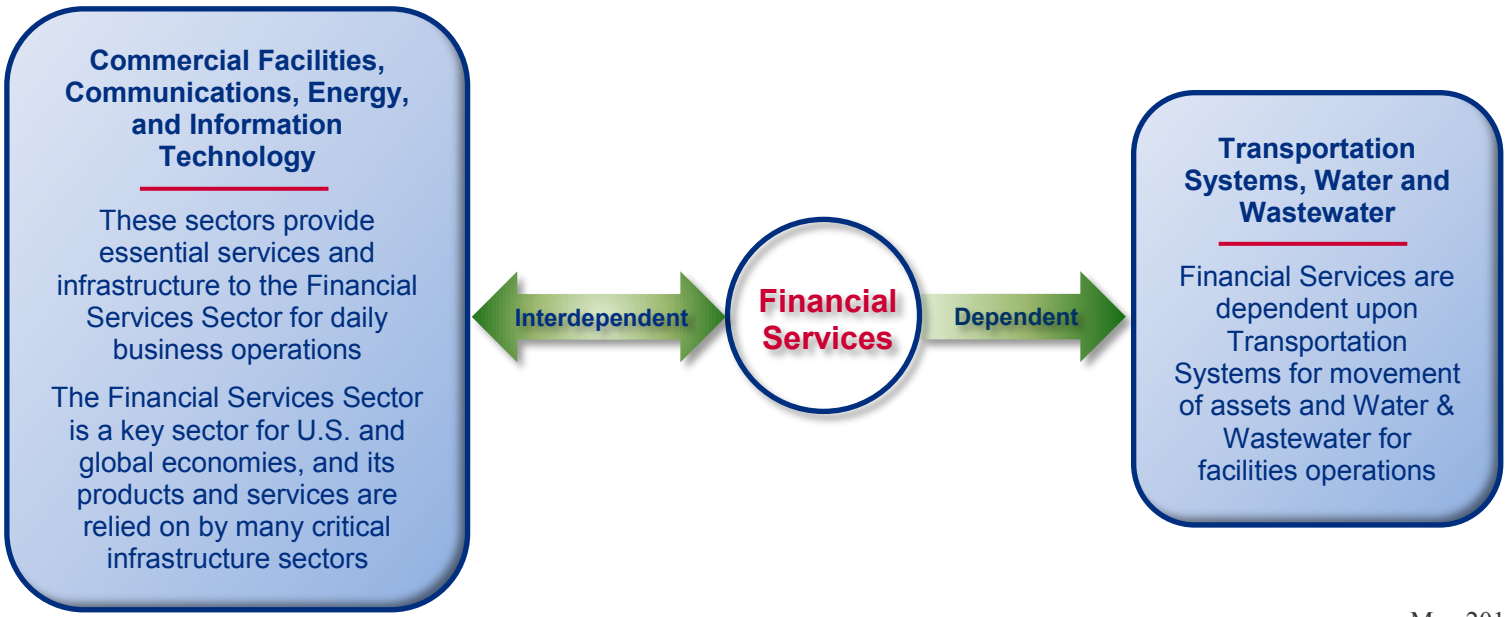
Threats and Hazards of Significant Concern

- **Cyberthreats**
  - Terrorists, transnational criminals, and foreign intelligence services are becoming aware of and using computer viruses, Trojan horses, worms, logic bombs, eavesdropping sniffers, and other tools that can destroy, intercept, degrade the integrity of, or deny access to data.
  - Other potential cyberthreats to the Sector include confidentiality and identity breaches, emerging technology, professionalization of cyber-criminals, and continued globalization of the Sector.
- **Insider Threats**
  - These threats could come from individuals or groups with malicious intent, including but not limited to disgruntled employees and organized crime members, or those with unwitting intent.
  - Insider threats pose a significant concern since these individuals often have knowledge that allows them to gain unrestricted access and inflict damage, steal, and/or move assets without possessing a great deal of knowledge about computer intrusions. Unwitting employees or third parties may also unintentionally damage, destroy, or steal data.
- **Large-scale Physical Events**
  - Natural hazards or terrorist attacks could cause significant economic losses to the Sector and to the Nation.
  - Regulators responsible for safety and soundness of financial services issue guidelines and specific regulations requiring redundancy and security in physical and financial systems. They have long required banking institutions to address operating and security risks in their contingency plans.

For More Information

- Sector-Specific Agency: Department of the Treasury, www.treasury.gov
- DHS, *National Risk Profile,* OCIA@hq.dhs.gov
- DHS, www.dhs.gov/banking-and-finance-sector
- Financial Services Information Sharing and Analysis Center (FS-ISAC), https://www.fsisac.com/

Figure 3: Common, First-order Dependencies and Interdependencies of the Financial Services Sector



May 2014

Homeland Security
Prepared by the DHS National Protection and Programs Directorate
Office of Cyber and Infrastructure Analysis (OCIA)
Questions or comments should be directed to OCIA@hq.dhs.gov

Homeland Security

Food and Agriculture Sector Sector Risk Snapshot

Food Defense

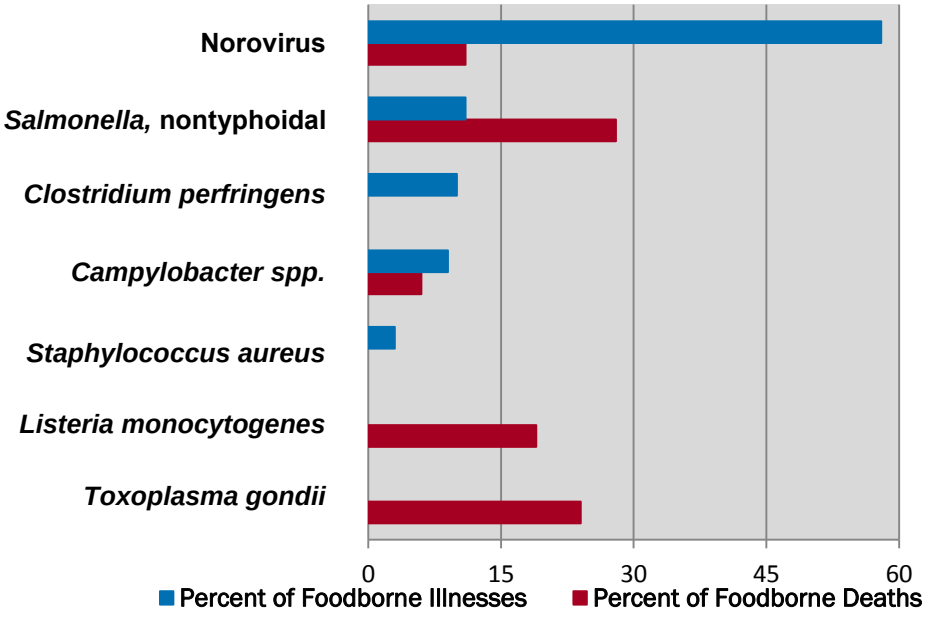
Activities associated with protecting the Nation's food supply from deliberate or intentional acts of contamination or tampering. This term encompasses other similar verbiage (e.g., bioterrorism or chemicalterrorism).

Food Safety

Activities associated with preventing the accidental contamination of food products by biological, chemical, or physical hazards. Focuses on the proper handling and preparation of food and agricultural products.

Figure 1: Top Pathogens Contributing to Domestically Acquired Foodborne Illnesses and Deaths, 2000-2008.

The Centers for Disease Control and Prevention (CDC) estimates that each year 1 in 6 Americans (or 48 million people) get sick, 128,000 are hospitalized, and 3,000 die of foodborne diseases.



Source: CDC, *2011 Estimates of Foodborne Illness in the United States*, www.cdc.gov/foodborneburden/2011-foodborne-estimates.html

Food And Agriculture Sector Overview

- **The Food and Drug Administration (FDA) and U.S. Department of Agriculture (USDA) jointly serve as the Sector Specific Agencies for the Food and Agriculture Sector.**
- **Composed of complex production, processing, and delivery systems and encompasses upwards of 4 million assets, including 2 million+ farms, 900,000+ restaurants, 100,000+ food retail establishments. As of February 19, 2014, there were 81,575 FDA registered domestic food facilities (warehouses, manufacturers, processors) and 115,753 FDA registered foreign food facilities. USDA regulates 6,805 establishments, including establishments for meat, poultry, processed egg products, imported products, and voluntary inspection services.**
- **Accounts for roughly one-fifth of the Nation's economic activity.**
- **The open nature and global interconnectivity of the sector presents unique security challenges, and leaves the sector vulnerable to a variety of all-hazards threats, including severe weather, pests and disease, and contamination with biological, chemical, or radiological agents.**
- **Direct attacks on the sector, such as the introduction of animal or plant disease, or deliberate food contamination, could result in devastating animal, plant, or public health and economic consequences.**

Food and Agriculture Infrastructure

- Food and Agriculture Sector infrastructure is unique, complex, broad-based, globally distributed, and highly integrated, and is seen as a system of systems (i.e., systems of individual assets that are closely dependent on each other).
- Many of the sector's systems defy traditional security practices because they are not brick-and-mortar entities, like buildings, bridges, or dams. Instead, they are open areas (i.e., farms, ranches, or livestock transport areas) and complex systems that span the globe.
- Many of these systems face natural threats, including livestock and crop diseases and foodborne pathogens, thus monitoring, early threat detection, and rapid response are key mitigation activities for the sector.
- Food and agriculture owners and operators must anticipate the possibility of a terrorist attack on their products and evaluate their preparedness and mitigation strategies to either thwart an attack or, at the very least, mitigate the damage, and recover from the animal, plant, public health, economic, and psychological impacts of an attack.

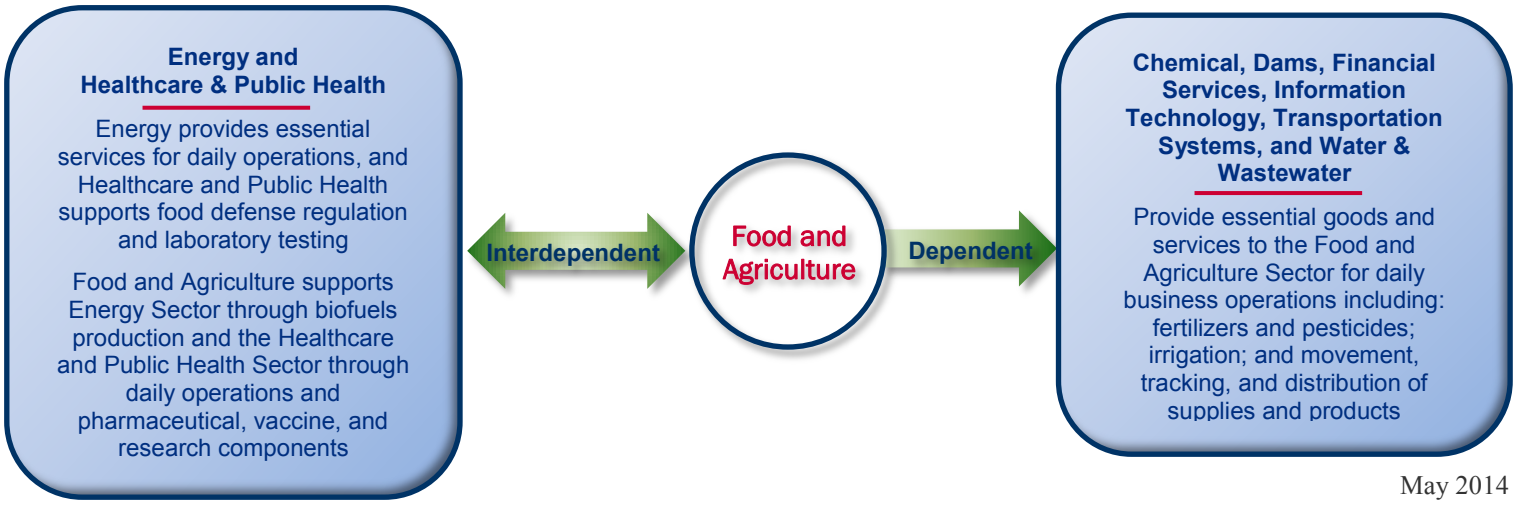
Threats and Hazards of Significant Concern

- **Food Contamination (whether by accidental or intentional means)**
  - Contaminated food in the United States is estimated to be responsible for over 47.8 million illnesses, 127,839 hospitalizations, and 3,037 deaths, costing the Nation more than $14 billion a year in terms of medical care, lost productivity, chronic health problems, and deaths (CDC, 2011).
  - Violent extremists and terrorists have indicated an interest in poisoning the food supply with biological and chemical agents, which has great potential to cause costly economic losses in the supply chain for implicated foodstuffs, creating public panic, and leading to a public health crisis with considerable mortality and morbidity (FBI, www.fbi.gov/stats-services/publications/law-enforcement-bulletin/february-2012/agroterrorism, 2012).
- **Disease and Pests**
  - The accessibility of crops and animals on the farm and the extensive international and interstate movement of animals and products increase the sector's vulnerability to rapidly spread disease.
  - Modeling estimates and historical evidence demonstrate that a domestic outbreak of a foreign animal disease, such as Foot and Mouth Disease, could cost the United States billions of dollars due to loss of livestock, production, and international trade.
- **Severe Weather (including droughts, floods, and climate variability)**
  - Natural hazards are an important risk to the Food & Agriculture Sector, and critically influence farm productivity.
  - Weather and climate characteristics such as temperature, precipitation, and water availability directly impact the health and well-being of plants and livestock, as well as pasture and rangeland production.
  - The harmful effects of severe weather coupled with global climate change are currently affecting U.S. water resources, agriculture, land resources, and biodiversity. This trend is expected to continue (USDA, 2013, www.usda.gov/oce/climate_change/effects.htm).

For More Information

- Sector-Specific Agencies: U.S. Department of Agriculture (USDA), Office of Homeland Security and Emergency Coordination, National Security Policy Staff, www.dm.usda.gov/ohsec/rpd/index.htm; and Department of Health and Human Services Food and Drug Administration (FDA), *Food Defense and Emergency Response*, www.fda.gov/Food/FoodDefense/default.htm
- DHS,www.dhs.gov/food-and-agriculture-sector
- DHS, *IP Note: Reducing the Vulnerability of the U.S. Food Supply to Intentional Contamination*, 10 August 2010
- DHS, USDA, FDA, *2010 Food and Agriculture Sector Specific Plan*, ww.dhs.gov/files/programs/gc_1179866197607.shtm
- DHS, *National Risk Profile,* OCIA@hq.dhs.gov

Figure 2: Common, First-order Dependencies and Interdependencies of the Food & Agriculture Sector



May 2014

Homeland Security

Prepared by the DHS National Protection and Programs Directorate
Office of Cyber and Infrastructure Analysis (OCIA)
Questions or comments should be directed to OCIA@hq.dhs.gov

Government Facilities Sector
Sector Risk Snapshot

Homeland Security

Government Facilities Security Levels

Because of the differences among Federal buildings and their security needs, U.S. Federal Marshals Services categorized Federal facilities into five classes based on building size, agency mission and function, tenant population, and the degree of public access to the facility, and developed security standards corresponding to the security level needed for each class.

Level I—buildings with no more than 2,500 square feet, 10 or fewer Federal employees, and limited or no public access

Level II—buildings with 2,500 to 80,000 square feet, 11 to 150 Federal employees, and moderate public access

Level III—buildings with 80,000 to 150,000 square feet or more, 151 to 450 Federal employees, and a moderate-to-high public access

Level IV—buildings with 150,000 square feet or more, more than 450 Federal employees, and a high level of public access

Level V—buildings that are similar to Level IV but are considered critical to national security

Critical Infrastructure Security and Resilience Issues

- Government facilities represent attractive and strategically important targets for both domestic and international terrorist groups, as well as criminals.
- These assets are often targeted because they provide unique services, often perform sensitive functions, and have significant symbolic value.
- Because of the high-profile nature of the sector, government facilities operate within a very dynamic risk environment requiring a variety of well-coordinated protective measures to ensure the safety and security of citizens and the continued availability of essential government functions.

Government Facilities Sector Overview

- **Comprises a wide variety of buildings, national monuments, and icons in the United States and overseas that are owned or leased by Federal, State, local, and tribal governments.**
- **The sheer size and scope of the Government Facilities Sector poses a challenge in providing for infrastructure protection efforts.**
- **The Federal Government alone manages approximately 3.35 billion square feet of space and more than 650 million acres of land across the United States. The Sector also includes the facilities owned and operated by the more than 87,000 municipal governments across the Nation and abroad.**
- **These facilities include general-use office buildings and special-use military installations, embassies, courthouses, and national laboratories that contain highly sensitive information, materials, processes, and equipment.**
- **Many government facilities are open to the public for business activities, commercial transactions, or recreational activities, while others are not.**
- **The Government Facilities Sector includes the Education Facilities Subsector, which covers pre-kindergarten through 12th grade schools, institutions of higher education, and business and trade schools.**
- **The National Monuments and Icons Subsector was consolidated within the Government Facilities Sector in 2013 under Presidential Policy Directive 21. The Subsector encompasses a diverse array of assets, networks, systems, and functions located throughout the United States. Many are listed in either the National Register of Historic Places of the List of National Historic Landmarks.**

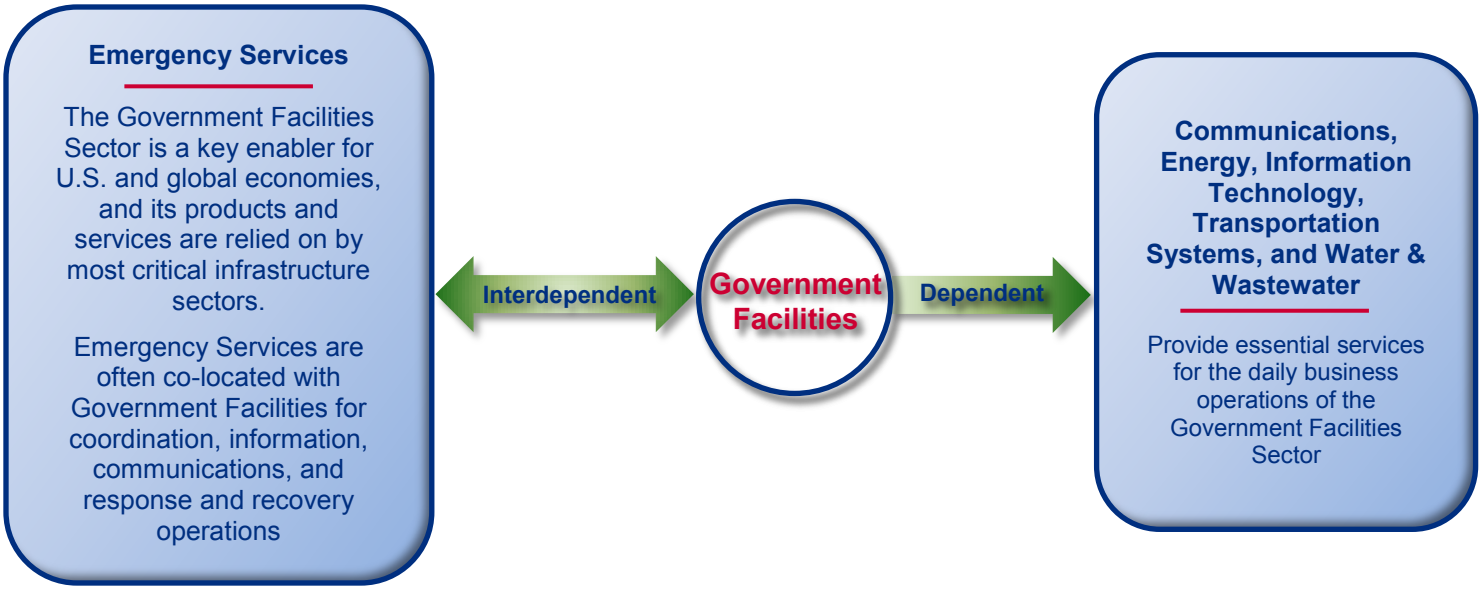
Threats and Hazards of Significant Concern

- **Terrorist Attacks**
  - The threat of terrorist attacks contributes significantly to the risks of the Government Facilities Sector. A major challenge in the protection of government facilities is balancing the need for security with the need for public access to government offices for services and transactions.
  - Global events and trends suggest that terrorists will likely continue to use improvised explosive device tactics—historically one of the most successful tactics—to attack U.S. critical infrastructure. Government facilities may also be targeted by active shooters, as occurred in the 2010 shooting at a Federal courthouse in Las Vegas. (Doherty, R., *Critical Research/Innovation Focus Area Document: Vehicle-Borne Improvised Explosive Devices (VBIED)* Detection, Washington, D.C.: U.S. Department of Homeland Security, Science and Technology Directorate, 2009)
- **Cyberthreats**
  - Cyberintrusions into automated security and supervisory control and data acquisition systems are risks. The increasing reliance on automated security systems and automated building management systems will likely increase vulnerabilities and the likelihood of cyberintrusion, especially in the form of sabotage by current or former insiders with malicious intent.
  - Cyberintrusion into the security systems of government facilities could compromise the protection of facilities, civil servants, and the general public and allow for exploitation and attacks with significant consequences.

For More Information

- Sector-Specific Agency: Department of Homeland Security Federal Protective Service www.dhs.gov/topic/federal-building-security, and the General Services Administration www.gsa.gov
- Government Facilities Sector, www.dhs.gov/government-facilities-sector
- National Infrastructure Protection Plan, www.dhs.gov/nipp
- DHS, *National Risk Profile*, OCIA@hq.dhs.gov
- Contact NIPP@hq.dhs.gov or NIPP-GFS@hq.dhs.gov

Figure 1: Common, First-order Dependencies and Interdependencies of the Government Facilities Sector



May 2014

Homeland Security

Prepared by the DHS National Protection and Programs Directorate
Office of Cyber and Infrastructure Analysis (OCIA)
Questions or comments should be directed to OCIA@hq.dhs.gov

The Principles of School Emergency Management Planning

Must be supported by leadership. At the district and school levels, senior-level officials can help the planning process by demonstrating strong support for the planning team.
Uses assessments to customize plans to the building level. Effective planning is built around comprehensive, ongoing assessment of the school community, which customizes plans to the building level, taking into consideration the school's unique circumstances and resources.
Considers all threats and hazards. The planning process must take into account a wide range of possible threats and hazards that may impact the school, addressing safety needs before, during, and after an incident.
Provides for the access and functional needs of the whole school community. The "whole school community" includes children, individuals with disabilities and others with access and functional needs, those from religiously, racially, and ethnically diverse backgrounds, and people with limited English proficiency.
Considers all settings and all times. School EOPs must account for incidents that may occur during and outside the school day as well as on and off campus (e.g., sporting events, field trips).
Creating and revising a model Emergency Operations Plan is done by following a collaborative process.

Source: U.S. Department of Education, Readiness and Emergency Managements for Schools Technical Assistance Center, http://rems.ed.gov/Default.aspx (2014).

Number of U.S. Educational Institutions by Number and Control of Institution

Public Schools (2012)	**98,328**
Elementary	66,689
Secondary	24,357
Combined	6,311
Other[1]	971
Private Schools (2011)	**30,860**
Postsecondary Title IV Institutions (2013)	**7,253**
Degree-granting institutions	4,726
2-year colleges	1,700
4-year colleges	3,026

[1]Includes special education, alternative, and other schools not classified by grade span

Source: U.S. Department of Education, National Center for Education Statistics, *2013 Digest of Education Statistics* (2014, Advance Release).

Education Facilities Subsector Overview

- **The Education Facilities Subsector (EFS) encompasses pre-kindergarten (pre-K) through 12th grade and post-secondary public, private, and proprietary education facilities.**
- **The Department of Education serves at the Sector-Specific Agency for the Education Facilities Subsector.**
- **EFS assets and systems vary dramatically and include rural and urban, public and private education facilities ranging from fewer than a hundred students to many thousands of students. EFS assets also include pre-K through 12 and higher education campus grounds, increasing the number of facilities, the level of complexity, and the challenges to risk mitigation.**
- **The overall EFS vision is that all education facilities are ready to prevent, mitigate, prepare for, respond to, and recover from any natural or manmade hazard, by having a comprehensive, all-hazards plan to enhance safety, minimize disruption, and ensure continuity of the learning environment.**
- **For the EFS, comprehensive, all-hazards emergency management plans are the appropriate approach to mitigating risk and enhancing resilience for all of EFS' human, physical, and cyber assets.**
- **Comprehensive plans are based on the four phases of school emergency management (prevention and mitigation, preparedness, response, and recovery). Such plans are practiced and updated regularly, coordinated with appropriate State and local partners, and developed in close collaboration with first responders and the community.**
- **They include written plans for an infectious disease outbreak, support the National Incident Management System, contain measures to address food defense, and incorporate students and staff with special needs.**

Threats and Hazards of Significant Concern

- **Natural Hazards** (e.g., hurricanes, wildfires)
  - Weather events pose a risk to the safety of the personnel and students at these institutions. Significant damage can cause the institution to close in the short and long term.
- **Public Health Hazards** (e.g., Methicillin-Resistant Staphylococcus Aureus (MRSA), salmonella outbreaks , H1N1, and intentional adulteration of food)
  - Public health hazards pose a risk to the safety of the personnel and students at these institutions. Significant damage can cause the institution to close in the short and long term.
- **Active Shooter** (e.g., Columbine, Virginia Tech, and Sandy Hook Elementary School)
  - Shootings pose a threat to the safety of the personnel and students at these institutions. Schools are targets because shootings bring national attention to the individual or group. Public confidence and the continuity of school operations could be negatively affected.
- **Cyberthreats** (e.g., computer system hacking, phishing)
  - Higher education institutions often collect and store sensitive, personal student data and databases (Social Security numbers, health, financial, and educational data). Education facilities with emergency management data housed electronically require cybersecurity efforts to maintain the integrity of their plans (i.e., emergency management plans, floor plans).
  - Disruptions to institutional data systems could impact the capacity to effectively perform essential business operations and could cause a temporary to long-term school closure.
  - Although a cyberattack on an education facility would not likely impose cascading effects for the Nation, it can have such effects on the campus community through the compromise of personal data, security systems, and research facilities that rely on cyber elements or of emergency management data housed electronically.

For More Information

- Sector-Specific Agency: The Department of Education, www.ed.gov
- DHS, *National Risk Profile*, OCIA@hq.dhs.gov
- DHS, 2010 Education Facilities Sector-Specific Plan, www.dhs.gov/xlibrary/assets/nipp-ssp-education-facilities-2010.pdf
- Readiness and Emergency Management for Schools, http://rems.ed.gov/

Figure 1: Common, First-order Dependencies of the Education Facilities Subsector

May 2014

Homeland Security

Prepared by the DHS National Protection and Programs Directorate
Office of Cyber and Infrastructure Analysis (OCIA)
Questions or comments should be directed to OCIA@hq.dhs.gov

Homeland Security

Healthcare and Public Health Sector Sector Risk Snapshot

Healthcare and Public Health Sector Overview

- **The Healthcare and Public Health (HPH) Sector is the lead Sector responsible for protecting and sustaining the Nation's health. The U.S. Department of Health and Human Services (HHS) serves as the Sector-Specific Agency for the HPH Sector.**
- **This widespread and diverse Sector includes acute care hospitals, ambulatory healthcare, public-private financial systems, Federal, State, and local public health systems; disease surveillance; and private sector industries that manufacture, distribute, and sell drugs, biologics, and medical devices.**
- **The Sector is vulnerable to a variety of all-hazards threats, and is especially concerned about potentially catastrophic impacts resulting from biological, cyber, vehicle-borne explosive devices, and insider threats.**
- **Such attacks could result in large numbers of illness and casualties, denial of service, or theft of confidential patient information.**
- **For the Sector, critical infrastructure protection is ultimately defined by the extent to which the Sector has been able to mitigate interruptions in the delivery of healthcare and public health services.**

Figure 1: Occurrence of Major Flu Pandemic or New Influenza Strain over the Past 100 years

Table 1: Major Flu Pandemics in the Past 100 Years, with Comparison to Seasonal Flu

	Virus Strain	First Identified	Ground Zero	Higher Risk/Age Group	Estimated Infection Rate	Mortality Rate	Estimated Deaths
Seasonal Flu	Seasonal variation	Seasonal variation	N/A	Very young, very old, and the infirm	5-15%	0.6%	0.25-0.5 million
Spanish Flu	H1N1	Spring 1918	Western Europe	Age 20-50	20-40%	2-2.5%	40-50 million
Asian Flu	H2N2	February 1957	China	School-aged children, elderly	30%	0.025%	2-4 million
Hong Kong Flu	H3N2	Early 1968	Hong Kong	Elderly	30%	0.02%	1-3 Million
Influenza A (H1N1)	H1N1	April 2009	Mexico	Children, teens, young adults	24%[1]	0.02%[1]	>18,500[1]

[1] World Health Organization (WHO), "Estimating age-specific cumulative incidence for the 2009 influenza pandemic: a meta-analysis of A(H1N1)pdm09 serological studies from 19 countries," *Influenza and Other Respiratory Viruses*, Vol:7, January 2013

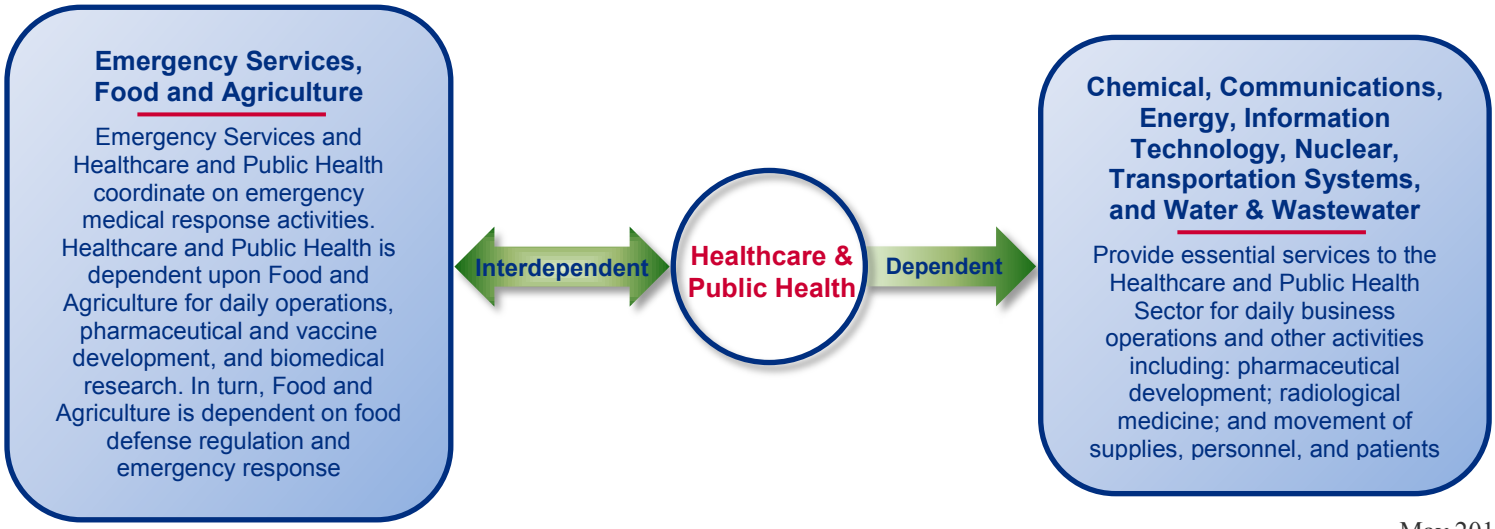
Threats and Hazards of Significant Concern

- **Global Supply Chain Disruptions**
  - A supply chain disruption refers to an event leading to a shortage of a pharmaceutical, device, or biologic. A natural disaster may make roads impassable and thereby prevent goods from arriving at an effected area, or a product may be contaminated at its place of origin and need to be recalled resulting in a limited amount of that product on the market.
  - Independent of the reason, supply chain disruptions can be catastrophic, as healthcare providers tend to rely on just-in-time resupplying and therefore do not always have sufficient stockpiles to weather a delay, especially during events that lead to an increased demand for healthcare or healthcare-related products.
- **Theft and Exploitation of Medical Goods and Confidential Medical Information**
  - Theft and exploitation result from the work of malicious actors.
  - Many medical facilities and laboratories contain radiological materials or biological select agents and toxins that are used for clinical treatment or medical research; and the open nature of these facilities presents a potential security vulnerability. These agents and materials may provide an attractive target to those wishing to construct a "dirty bomb," intentionally infect a population, or sell the material on the black market.
  - Medical systems and vital records are also at risk for compromise or theft by external hackers or malicious insiders, and cybertheft presents a trend in medical identity theft.
- **Pandemic**
  - Recent experience with influenza demonstrated how a rapidly-spreading infectious agent can significantly impact the HPH Sector and the country as a whole. A naturally occurring agent like influenza was able to cause death, hospitalizations, and absenteeism.
  - If a more dangerous agent, such as smallpox, were intentionally released, the effects could be even more catastrophic due to the increased lethality and our general immunological naiveté to the disease.

For More Information

- Sector-Specific Agency: Department of Health and Human Services (HHS), Public Health Preparedness and Emergency, www.phe.gov
- DHS, HHS, *2010 Healthcare and Public Health Sector-Specific Plan*, www.dhs.gov/files/programs/gc_1179866197607.shtm
- DHS, *National Risk Profile,* OCIA@hq.dhs.gov

Figure 2: Common, First-order Dependencies and Interdependencies of the Healthcare and Public Health Sector



May 2014

Homeland Security

Prepared by the DHS National Protection and Programs Directorate
Office of Cyber and Infrastructure Analysis (OCIA)
Questions or comments should be directed to OCIA@hq.dhs.gov

Homeland Security

Information Technology Sector
Sector Risk Snapshot

Critical IT Sector Functions

- IT products and services
- Incident management capabilities
- Domain name resolution services
- Identity management and associated trust support services
- Internet-based content, information, and communications services
- Interrouting, access, and connection services

Information Technology Sector Overview

- Businesses, governments, academia, and private citizens are increasingly dependent upon IT Sector functions. The Information Technology (IT) Sector is central to the Nation's security, economy, public health, and safety.
- These virtual and distributed functions produce and provide hardware, software, IT systems and services, and—in collaboration with the Communications Sector—the Internet.
- The Sector's complex and dynamic environment makes identifying threats and assessing vulnerabilities difficult, and requires that these tasks be addressed in a collaborative and creative fashion.
- The IT Sector functions are operated by a collaboration of entities—often owners and operators and their respective associations—that maintain and reconstitute the network, including the Internet.
- Although the IT infrastructure has a certain level of inherent resilience, its interdependent and interconnected structure presents challenges as well as opportunities for coordinating public and private sector preparedness and protection activities.
- The IT Sector is at constant risk from cyberthreats, and identifying threat actors, intrusion methods, and network vulnerabilities are critical to mitigation and longer-term defensive strategies (Figure 1 and 2).

Figure 1: 2012 Confirmed Data Breach and Network Intrusion Threat Actors

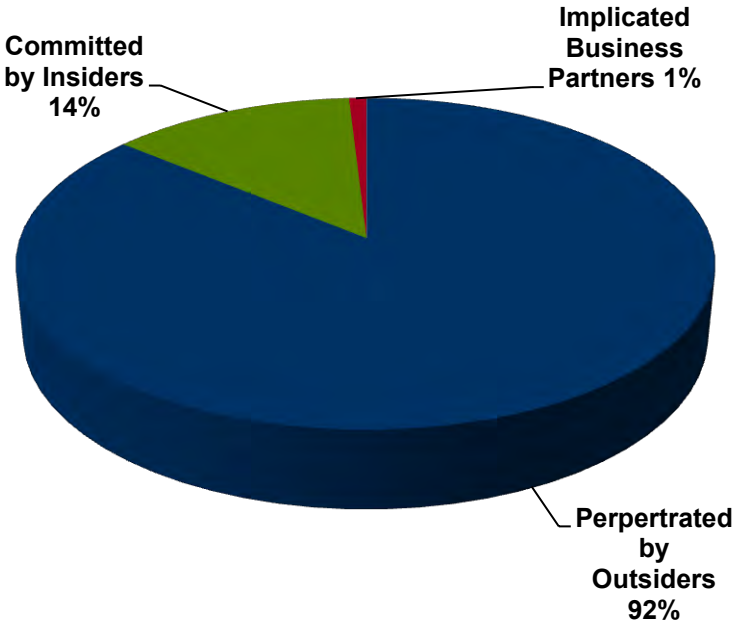
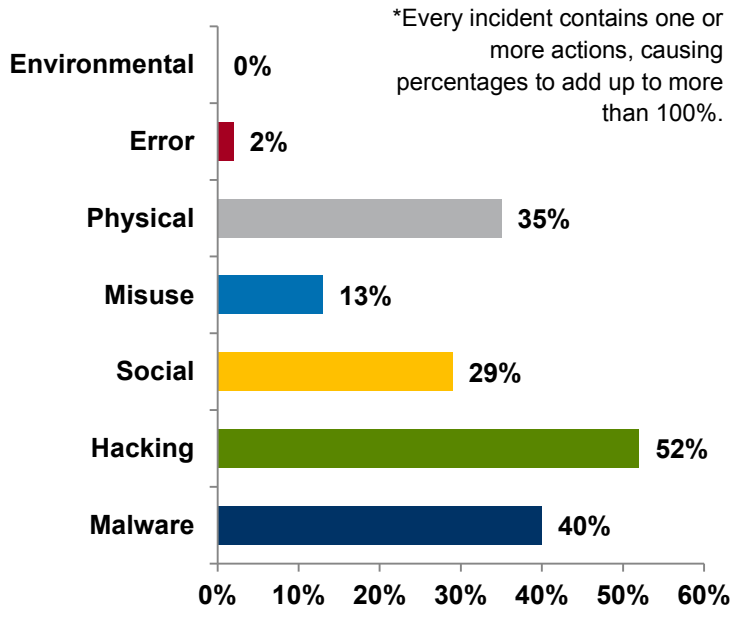


Figure 2: 2012 Confirmed Data Breach and Network Intrusion Threat Actions



Source: Verizon, *2013 Data Breach Investigations Report*, www.verizonenterprise.com/DBIR/2013/

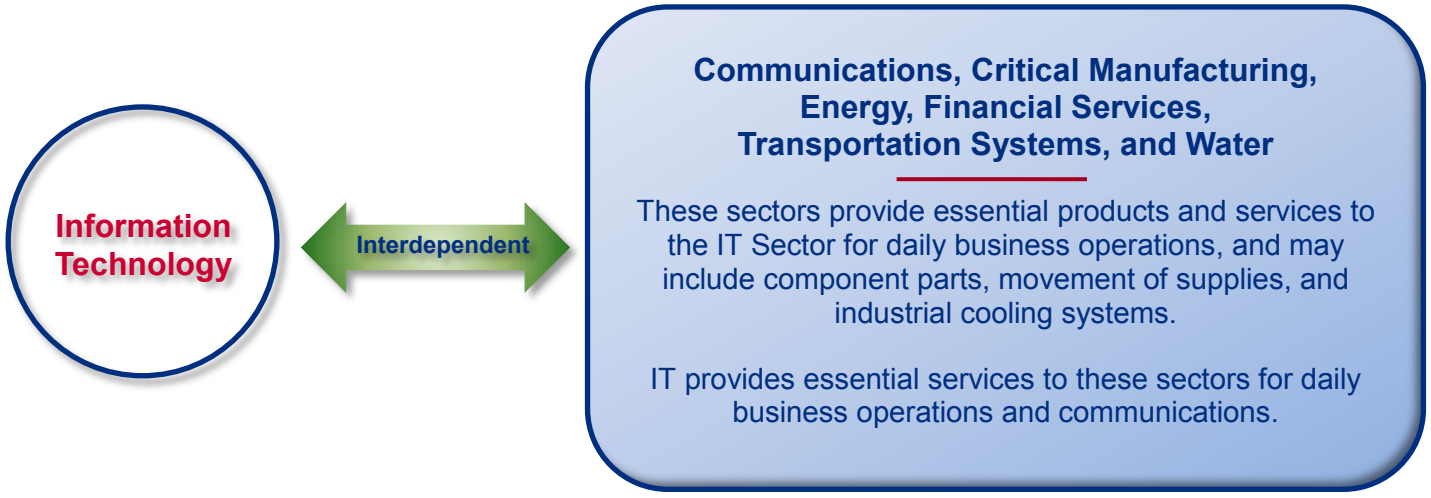
Threats and Hazards of Significant Concern

- **Cyberthreats**
  - The IT Sector is highly concerned about cyberthreats, particularly those that degrade the confidentiality, integrity, or availability of the Sector's critical functions.
  - Depending on its scale, a cyberattack could be debilitating to the IT Sector's highly interdependent critical infrastructures and ultimately to the Nation's economy, homeland security, and national security.
  - These cyberthreats include unintentional acts (e.g., the accidental disruption of Internet content services) and intentional acts (e.g., the exploitation of IT supply chain vulnerabilities or the loss of interoperability between systems as the result of an attack).
- **Attacks Targeting Internet-based Identity**
  - These include attacks targeting management, content, information, and communications. For example, malicious code increasingly proliferates through social networking and can degrade information technology system functionality.
  - Failures in identity management systems can lead to serious consequences like identity theft, criminal activity, unauthorized access to sensitive or classified information, systems, and facilities, which could jeopardize public safety and the operation of financial, government, or law enforcement systems.

For More Information

- Sector-Specific Agency: DHS, Office of Cybersecurity and Communications, www.dhs.gov/office-cybersecurity-and-communications
- DHS IT Sector, www.dhs.gov/information-technology-sector
- DHS, *National Risk Profile*, OCIA@hq.dhs.gov
- U.S. Cyber Emergency Readiness Team, www.us-cert.gov
- U.S. Industrial Control Systems Cyber Emergency response Team (ICS-CERT), ics-cert.us-cert.gov
- National Vulnerability Database, http://nvd.nist.gov
- FBI Cyber Crime Investigations, www.fbi.gov/about-us/investigate/cyber

Figure 3: Common, First-order Interdependencies of the IT Sector



May 2014

Homeland Security

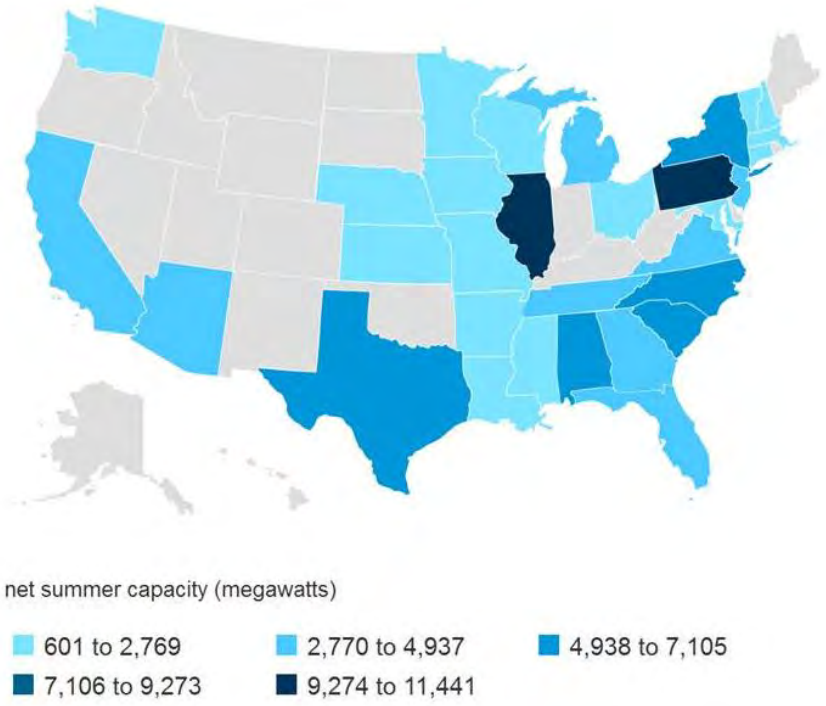
Prepared by the DHS National Protection and Programs Directorate
Office of Cyber and Infrastructure Analysis (OCIA)
Questions or comments should be directed to OCIA@hq.dhs.gov

Homeland Security

Nuclear Reactors, Materials, & Waste Sector

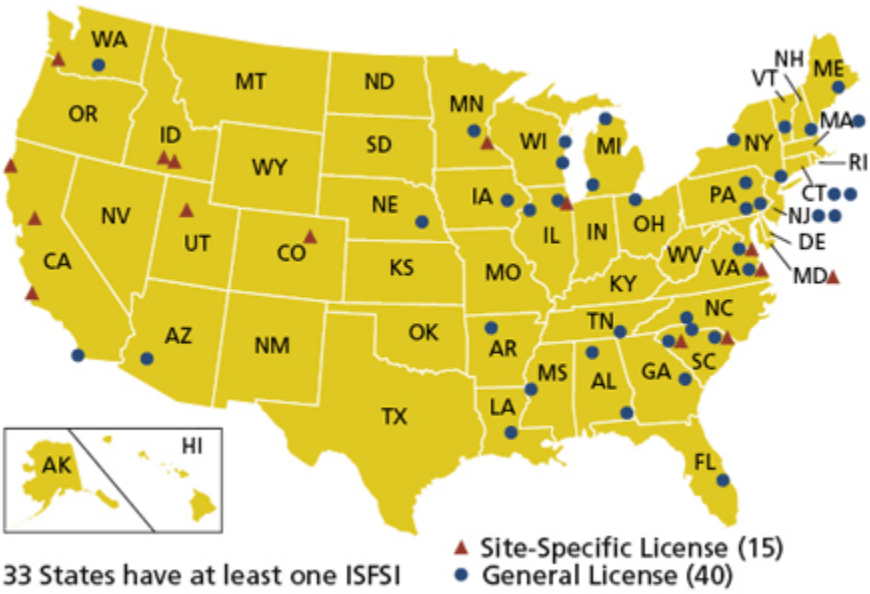
Sector Risk Snapshot

Figure 1: U.S. Nuclear Capacity and Generation



Source: U.S. Energy Information Administration (EIA), *Nuclear and Uranium*, 2014, www.eia.gov/nuclear/state.

Figure 2: Licensed/Operating Independent Spent Fuel Storage Installations



Source: U.S. Nuclear Regulatory Commission, *Locations of Independent Spent Fuel Storage Installations,* 2012, www.nrc.gov/waste/spent-fuel-storage/locations.html.

Nuclear Sector Overview

- Comprises nuclear power plants; research and test reactors; fuel cycle facilities; radioactive waste management; decommissioning reactors; nuclear and radioactive materials used in medical, industrial, and academic settings; and nuclear material transport.
- 104 nuclear power reactors at 65 nuclear power plants account for nearly 20 percent of annual U.S. electricity production (Figure 1). Increases in nuclear generation have roughly tracked the growth in total electricity output.
- There are 31 research and test reactors nationwide. Also known as non-power reactors, they are used primarily for education and research and development.
- Radioactive materials, including more than 75,000 high-activity sources, are used daily in a range of industrial, medical, and other commercial settings.
- The Sector faces current and ongoing risk for Sector facilities and materials due to physical incidents, cyber-disruptions, theft, diversion of materials, and disruptions in the supply chain.
- Theft or diversion of nuclear materials would pose a significant risk to populations through mishandling of the material or the use of a radiological dispersal device (RDD) or, in the worst case, the detonation of an improvised nuclear device.
- If successfully attacked or disrupted, some nuclear facilities have the potential to release radioactive material into the environment.

Radioactive Waste

- Most spent nuclear fuel is safely stored in specially designed pools at individual reactor sites around the country (Figure 2).
- Licensees may move spent fuel rods to above-ground dry storage casks after a minimum 5-year decay period, and if the licensee has an approved above-ground dry storage facility.

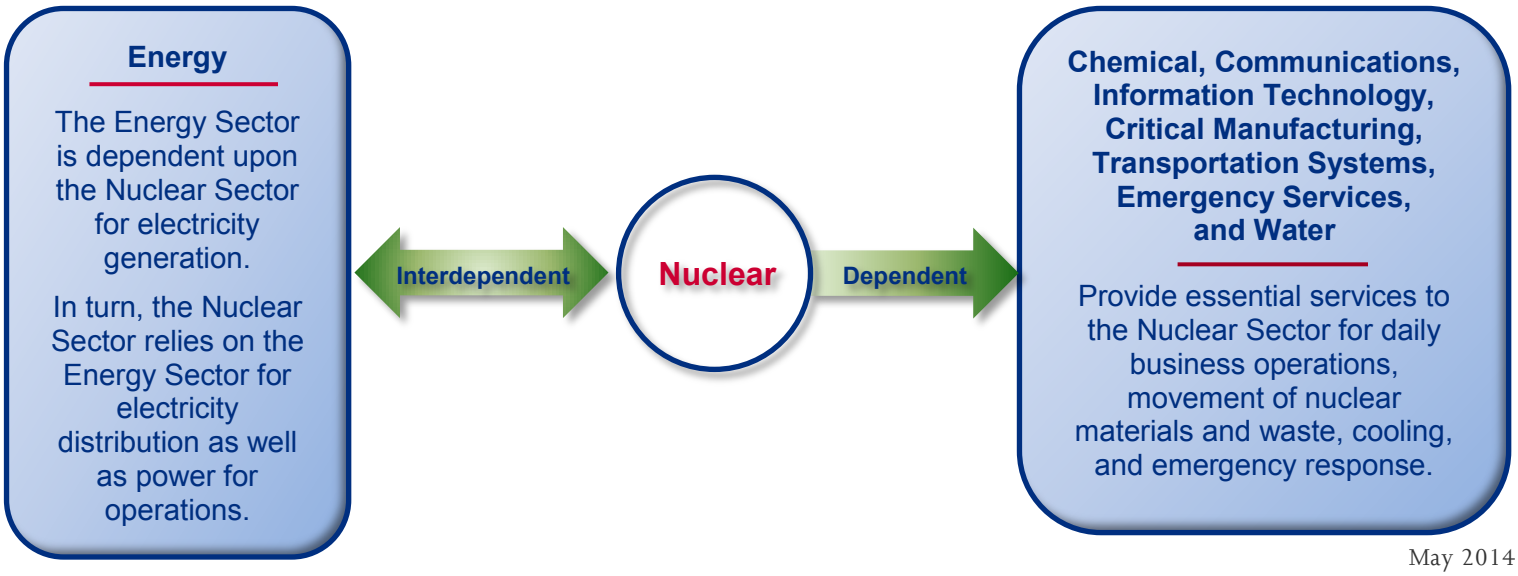
Threats and Hazards of Significant Concern

- **Theft and diversion of nuclear and radioactive materials:**
  - Determined and skilled adversaries could use stolen radioactive materials as elements of improvised nuclear devices (IND), radiological dispersion devices (RDD), or radiological exposure devices.
- **Natural hazards (e.g. hurricanes, tornados, floods, earthquakes, and drought):**
  - Pose a serious and continuing risk for the Sector.
  - The loss or disruption of a single nuclear power plant would have limited impact on the Nation's overall electrical capacity.
  - Sector infrastructure may be severely disrupted or destroyed by such hazards, which may further complicate an overall disaster emergency response due to multiple cross-sector interdependencies (Figure 3).
- **Physical and cyberattacks on Nuclear Sector infrastructure and assets by terrorists, homegrown extremists, or disgruntled insiders:**
  - Physical attacks using improvised explosive devices on nuclear power reactors, spent fuel and radioactive waste storage facilities, and fuel cycle facilities could result in a release of hazardous materials.
  - Cyberattacks and intrusions on industrial control systems may pose a significant threat to the Sector, allowing malicious actors to manipulate or exploit facility operations.

For More Information

- Sector-Specific Agency: DHS, Office of Infrastructure Protection, www.dhs.gov/about-office-infrastructure-protection
- Nuclear Regulatory Commission, www.NRC.gov
- Nuclear Energy Institute, www.NEI.org
- DHS, *National Risk Profile,* OCIA@hq.dhs.gov
- DHS, 2010 Nuclear Reactors, Materials, and Waste Sector-Specific Plan, www.dhs.gov/files/programs/gc_1179866197607.shtm

Figure 3: Common, First-order Dependencies and Interdependencies of the Nuclear Sector



May 2014

Homeland Security

Prepared by the DHS National Protection and Programs Directorate
Office of Cyber and Infrastructure Analysis (OCIA)
Questions or comments should be directed to OCIA@hq.dhs.gov

Homeland Security

Aviation Mode
Transportation Sector

Sector Risk Snapshot

Figure 1: Major Continental U.S. Airport Locations

Table 1: Schedules System (Domestic and International) Airline Travel on U.S. Airlines

	2012	2013	Change %
Passengers (in millions)	736.7	743.1	0.9
Flights (in thousands)	9,287.40	7,158.70	-1.4
Revenue Passenger Miles (in billions)	823.2	840.4	2.1
Available Seat-miles (in billions)	994.5	1.011.20	1.7
Load Factor*	82.8	83.1	0.3
Flight Stage Length**	755	770.3	2
Passenger Trip Length***	1,117.40	1,131.00	1.2

Source: Bureau of Transportation Statistics, *T-100 Market and Segment*, March 13, 2014, www.rita.dot.gov/bts/press_releases/bts012_14
* Measure of the amount of utilization of the total available capacity of an airline, i.e. percent of available seat-miles (ASM) occupied by passengers
** The average non-stop distance flown per departure in miles
*** The average distance flown per passenger in miles
Note: Percentage changes based on numbers prior to rounding.

Aviation Mode Overview

- **The Aviation Transportation System (ATS) is a vital mode within the Transportation Sector, integrally contributing to the free flow of people and commerce across the globe.**
- **The Aviation Mode consists of more than 19,700 airports in the United States. Of these, 5,170 are open to the general public with 503 offering commercial service.**
- **The ATS includes more than 690 air traffic control facilities, and over 11,000 air navigation facilities.**
- **More than 780,000 passenger flights take place over the United States each month carrying nearly 60 million passengers.**
- **This Mode transports more than 13 million ton-miles of freight domestically each year.**
- **The security and economic prosperity of the United States depend significantly upon the secure operation of its ATS and safe use of the world's airspace.**
- **Significant threats to the ATS include the potential for terrorist infiltrations and attacks, cyber attacks against ATS assets, and the hostile exploitation of air cargo.**
- **The U.S. Department of Homeland Security (DHS), Department of Transportation (DOT), and Department of Defense (DOD) continue to develop and enhance technological and procedural measures to detect, prevent, respond to, mitigate and recover from physical and cyber-based attacks on the ATS's critical infrastructure.**

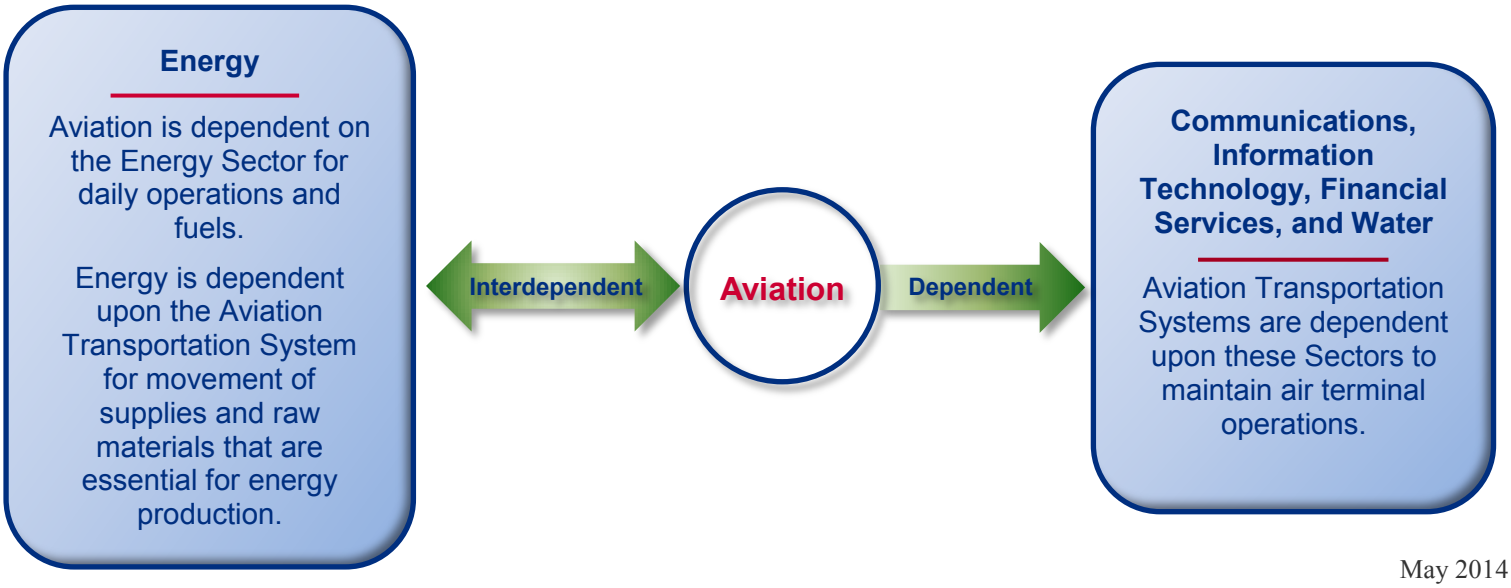
Threats and Hazards of Significant Concern

- **Terrorism**
  - Terrorism threats to the ATS persist. Aircraft have been the primary target of attacks in the past, and have been used as weapons. Despite security enhancements made after the attacks on September 11, 2001, intelligence continues to indicate that aviation remains a top target of terrorists. (DHS and TSA, 2011)
  - Terrorist groups are adapting to aviation countermeasures in multiple ways, including modality of planning, complexity of potential attacks, and methods of attack execution.
- **Cyberthreats**
  - The Sector focuses on developing countermeasures to address specific risks in the cyber-realm. A concerted, well-orchestrated attack on any Sector cybernetwork could cause considerable disruption Sector-wide.
  - The Federal Aviation Administration is collaborating with industry, academia, and other Federal agencies on aircraft cybersecurity research and development *(https://faaco.faa.gov/index.cfm/announcement/view/14453)*.
- **Cargo**
  - The air-cargo industry is highly dynamic and encompasses a wide range of users, characteristics which expose it to exploitation by terrorists.
  - Terrorists may use unsecured air transportation routes to transport arms, explosives, or operatives clandestinely to safe havens, training sites, or attack-staging locations. Ultimately, terrorists may use these access points and routes to transport more dangerous cargo, including weapons of mass destruction and their associated components.

For More Information

- Sector-Specific Agency: DHS, Transportation Security Administration (TSA), www.tsa.gov, Department of Transportation, www.dot.gov
- Federal Aviation Administration, www.faa.gov
- DHS, *National Risk Profile*, OCIA@hq.dhs.gov
- DHS and TSA, *2010 Transportation Sector-Specific Plan*, www.dhs.gov/xlibrary/assets/nipp-ssp-transportation-systems-2010.pdf

Figure 2: Common, First-order Dependencies and Interdependencies of the Aviation Mode



May 2014

Homeland Security

Prepared by the DHS National Protection and Programs Directorate
Office of Cyber and Infrastructure Analysis (OCIA)
Questions or comments should be directed to OCIA@hq.dhs.gov

Homeland Security

Freight Rail Mode
Transportation Sector

Sector Risk Snapshot

Figure 1: The rail network accounts for approximately 40 percent of U.S. freight moves by ton-miles (the length freight travels)
Source: Federal Railroad Administration, "National Rail Plan Progress Report," 2010

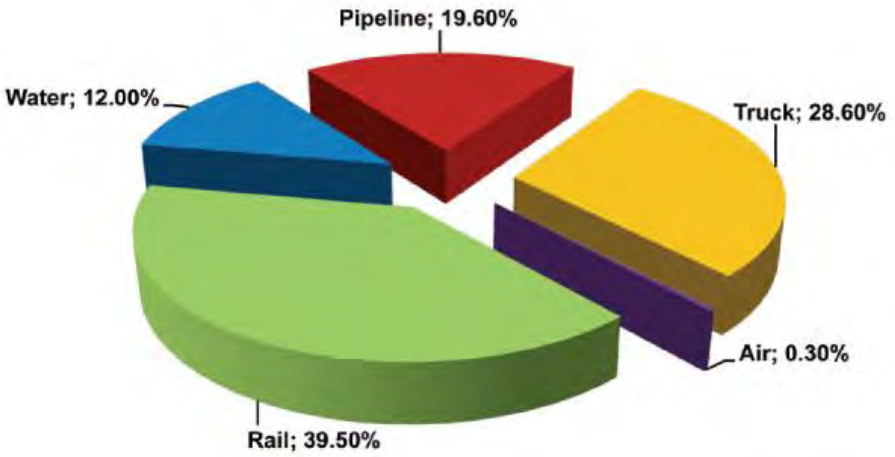
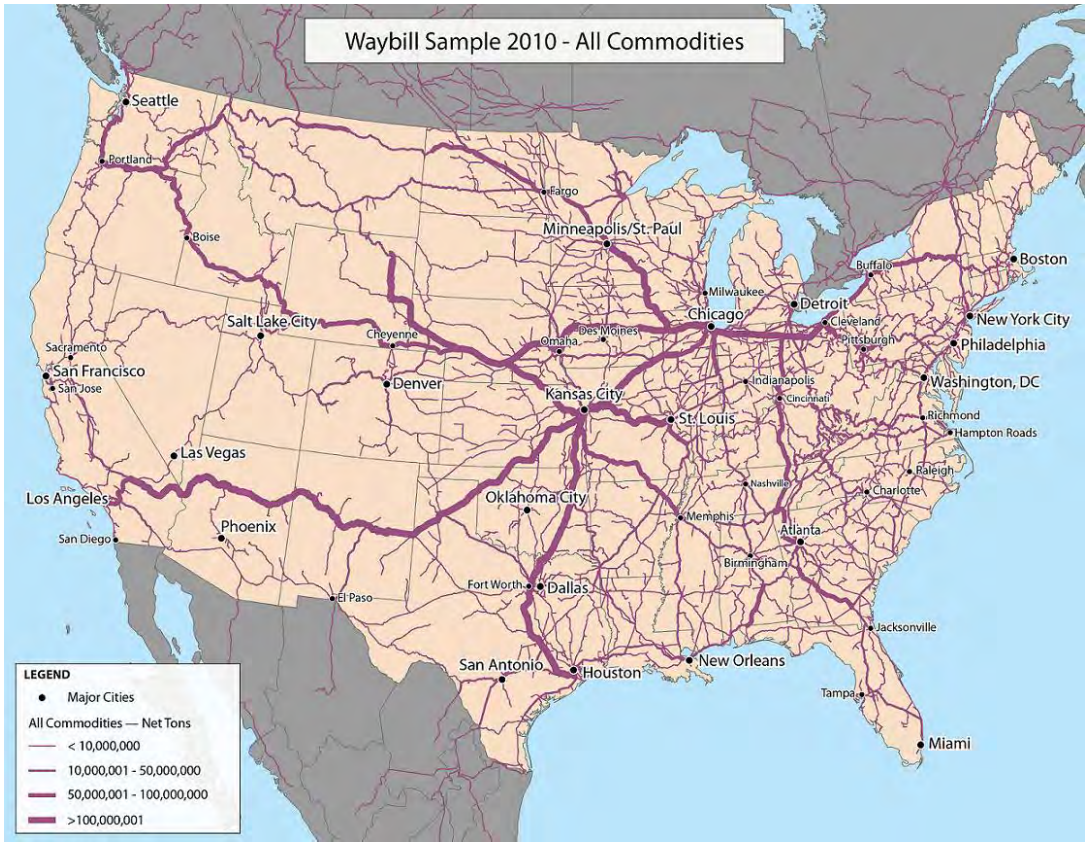


Figure 2: U.S. Freight Rail System Map
Source: Federal Railroad Administration, based on Surface Transportation Board's 2010 Carload Waybill Sample



Freight Rail Mode Overview

- **Freight Rail is one of seven modes that make up the Transportation Sector.**
- **The $60 billion industry consists of 140,000 miles of active rail track and provides 221,000 jobs across the country.**
- **Passenger and commuter rail systems throughout the country operate at least partially over tracks or rights-of-way owned by freight railroads. The National Railroad Passenger Corporation (Amtrak), for example, operates on more than 22,000 miles of track owned by freight railroads.**
- **Freight rail comprises 565 carriers divided among 3 Classes: Class I are the 7 major long haul carriers responsible for approximately 93 percent of total Sector revenue; the remaining 558 carriers (Class II and III) are local or short-haul carriers.**
- **Freight rail plays a critical role in support of the Energy Sector. Freight railroads are responsible for the transportation of more than 70 percent of all U.S. coal shipments (7.0 million carloads in 2010). Coal is the fuel that generates half of America's electricity.**

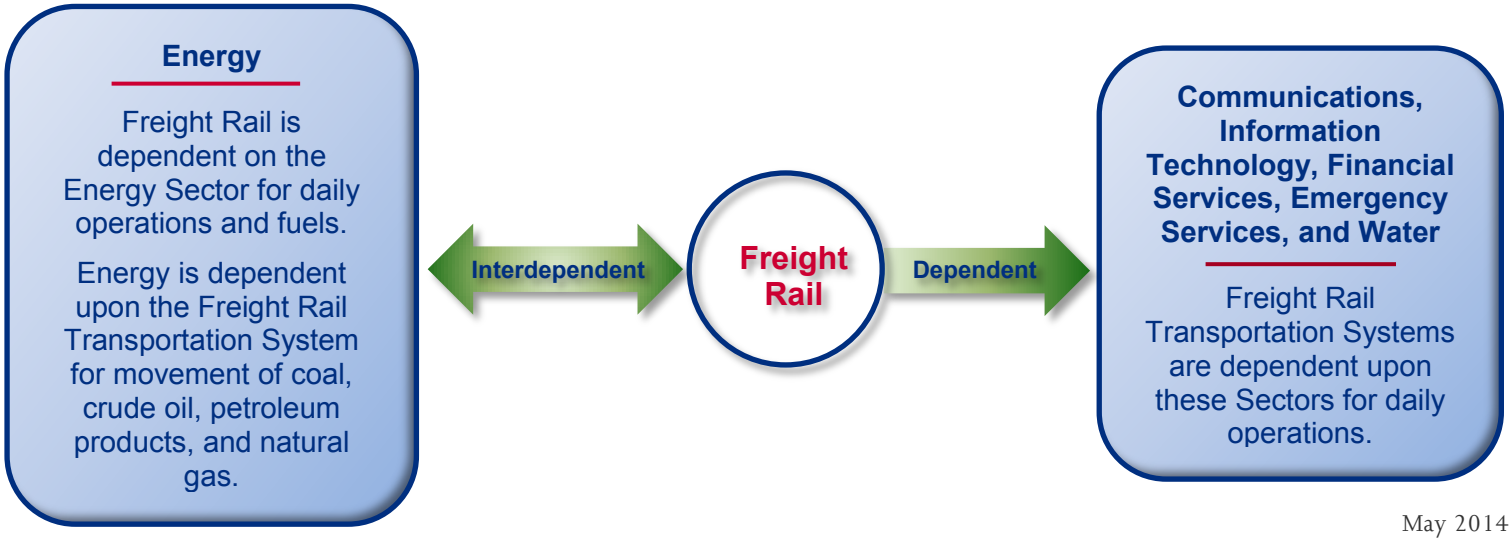
Threats and Hazards of Significant Concern

- **Sensitive Freight and Access Points**
  - Transportation Security Administration's (TSA's) risk assessment efforts examine the critical assets (e.g., bridges, tunnels, and yards) required for carrying out the freight railroad's basic mission of moving freight. Rail yards and terminals represent the fixed points in the network of railroad assets at which cars are transferred from one train to another, inspected, and repaired as necessary.
  - The movements of security-sensitive materials and toxic inhalation hazard materials through freight rail facilities, or over open tracks, leave railroad employees and public populations vulnerable if confronted with the threat of a terrorist attack.
- **Terrorist Attacks**
  - Intelligence reviews of various attacks worldwide, as well as analysis of seized documents, and the interrogation of captured and arrested suspects, reveal that there has been historic interest in carrying out attacks on railroad systems, particularly passenger rail systems due to the potential for large civilian casualties.
  - TSA concludes that long stretches of open, unattended track and numerous critical points (e.g., junctions, bridges, contiguous passenger rail sites) that are difficult to secure make the U.S. freight rail system an attractive target for terrorist attacks.
- **Insider Threat**
  - While the risk is considered low to moderate, documented evidence shows that disgruntled persons have tampered with tracks and other rail components.
  - Control systems are also vulnerable to tampering or external cyberattacks. However, the fail-safe nature of freight rail control systems may serve to mitigate the risk of a catastrophic incident.

For More Information

- Sector-Specific Agencies: DHS, Transportation Security Administration (TSA), www.tsa.gov, Department of Transportation, www.dot.gov
- Federal Rail Administration, www.fra.dot.gov
- American Association of Railroads, www.aar.org
- DHS, *National Risk Profile*, OCIA@hq.dhs.gov
- DHS and TSA, 2010 Transportation Sector-Specific Plan, www.dhs.gov/xlibrary/assets/nipp-ssp-transportation-systems-2010.pdf

Figure 3: Common, First-order Dependencies and Interdependencies of the Freight Rail Mode



May 2014

Homeland Security

Prepared by the DHS National Protection and Programs Directorate
Office of Cyber and Infrastructure Analysis (OCIA)
Questions or comments should be directed to OCIA@hq.dhs.gov

Homeland Security

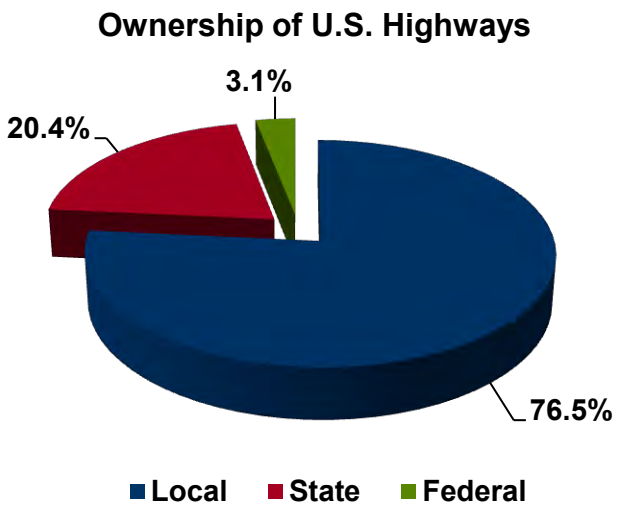
Highway and Motor Carrier Mode
Transportation Sector

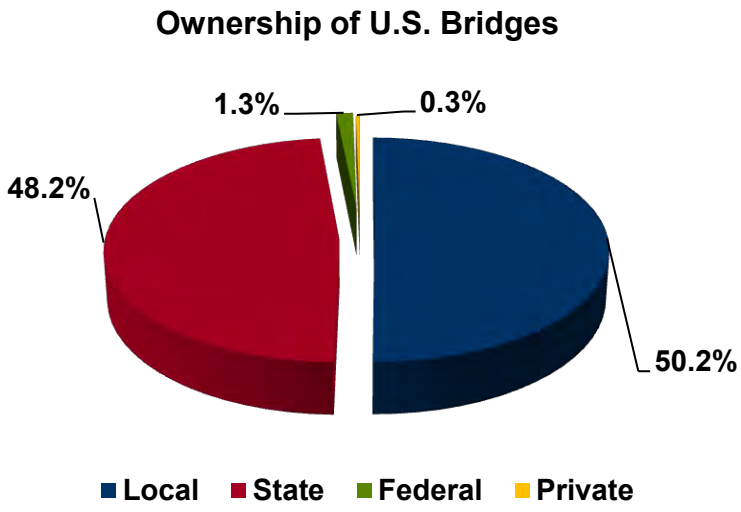
Sector Risk Snapshot

Highway and Motor Carrier Mode Overview

- **The Highway & Motor Carrier Mode assets include, but are not limited to, bridges, major tunnels, operations and management centers, trucks carrying hazardous materials, other commercial freight vehicles, motor coaches, school buses, and key intermodal facilities.**
- **The trucking industry is unique in that it is the only segment of the Highway Mode with complete intermodal supply chain relationships with aviation, maritime, mass transit, freight rail, and pipeline.**
- **The Nation's highway network includes nearly 4 million miles of roadway, almost 600,000 bridges, and some 400 tunnels.**
- **This Mode faces current and ongoing risk to facilities and materials due to terrorist attacks, natural hazards, and cyber-incidents.**
- **If successfully attacked or disrupted, impacts could result in regional shutdowns, diversions, or costly repairs with potentially severe results.**

Figure 1: Ownership of U.S. Highways and Bridges (2010)
Source: Department of Transportation, Federal Highway Administration, 2013 *Status of the Nation's Highways, Bridges, and Transit: Conditions & Performance*, January 31, 2014, www.fhwa.dot.gov/policy/2013cpr/overviews.htm





Hazardous Materials

- **The Transportation Security Administration (TSA) Hazardous Materials Endorsement Threat Assessment Program conducts a security threat assessment for any driver seeking to obtain, renew, or transfer a hazardous materials endorsement on a state-issued commercial driver's license.**
- **Hazardous materials include poisonous vapors, aerosols, liquids, and solids that have toxic effects on people, animals, or plants.**
- **They can have an immediate effect (a few seconds to a few minutes) or a delayed effect (2 to 48 hours).**
- **While potentially lethal, chemical agents are difficult to deliver in lethal concentrations. Outdoors, the agents often dissipate rapidly.**

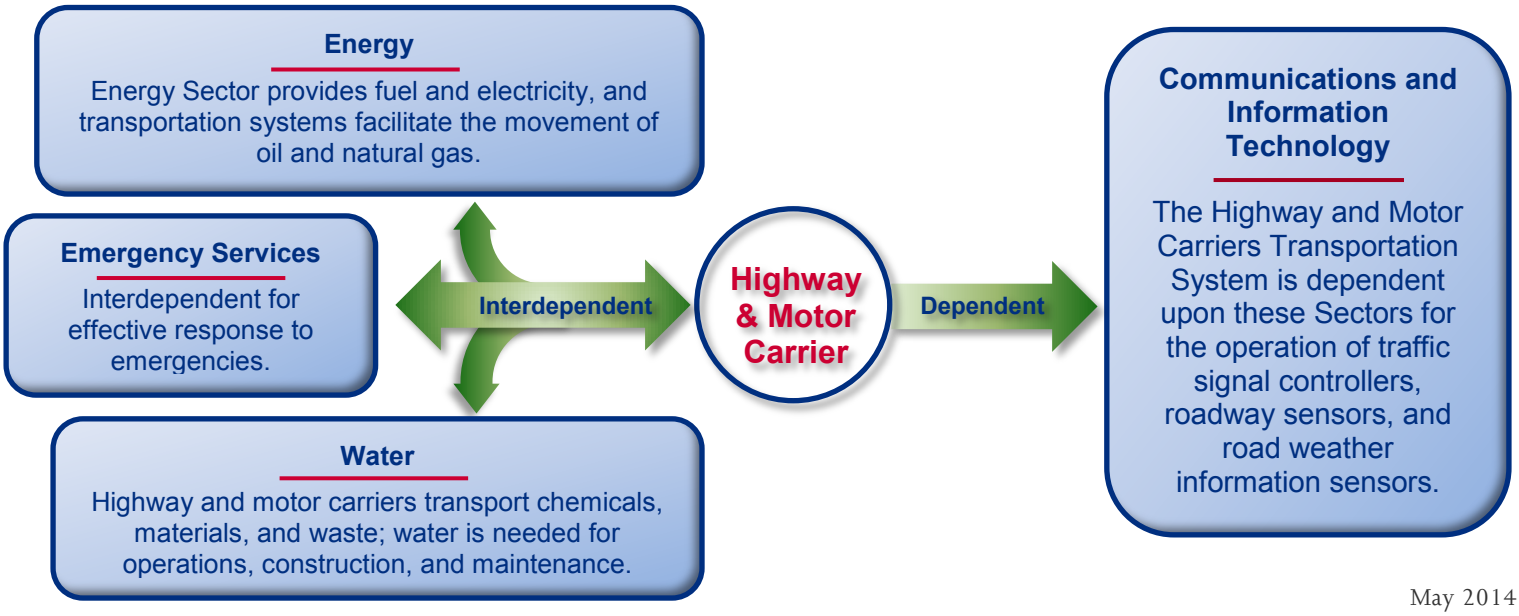
Threats and Hazards of Significant Concern

- **Terrorist attacks involving highway infrastructure and assets**
  - Highway infrastructure and assets may either be a target [e.g., improvised explosive devices (IEDs) against highway structures] or serves as a means to conduct an attack against other targets (e.g. use of a truck as a vehicle-borne IED against a building).
  - Use of HAZMAT materials as a terrorist attack is a serious and continuing risk to the Highway Mode.
- **Natural hazards, such as hurricanes, tornadoes, floods, and earthquakes**
  - Highway infrastructure may be severely disrupted or destroyed by such hazards, which may further complicate an overall disaster emergency response due to multiple cross-sector interdependencies.
- **Cyberattacks on highway infrastructure by terrorists, homegrown extremists, or disgruntled insiders**
  - Cyberattacks and intrusions on traffic control systems or other business systems pose a serious threat to highway infrastructure allowing malicious actors to manipulate or exploit control systems essential to operation of traffic control systems and highway messaging systems.

For More Information

- Sector-Specific Agency: DHS, Transportation Security Administration (TSA), www.tsa.gov, Department of Transportation, www.dot.gov
- American Association of State Highway and Transportation Officials, http://transportation.org/default.html
- American Bus Association, www.buses.org
- American Trucking Association, www.trucking.org/Pages/Home.aspx
- Federal Highway Administration, www.fhwa.dot.gov
- Pipeline and Hazardous Materials Safety Administration, http://phmsa.dot.gov/hazmat
- DHS, *National Risk Profile,* OCIA@hq.dhs.gov
- DHS and TSA, *2010 Transportation Sector-Specific Plan*, www.dhs.gov/xlibrary/assets/nipp-ssp-transportation-systems-2010.pdf

Figure 2: Common, First-order Dependencies and Interdependencies of the Highway and Motor Carrier Mode



May 2014

Homeland Security

Prepared by the DHS National Protection and Programs Directorate
Office of Cyber and Infrastructure Analysis (OCIA)
Questions or comments should be directed to OCIA@hq.dhs.gov

Homeland Security

Maritime Mode Transportation Sector Sector Risk Snapshot

Figure 1: U.S. Import Value by Mode of Transportation, 2011, in Millions of U.S. Dollars

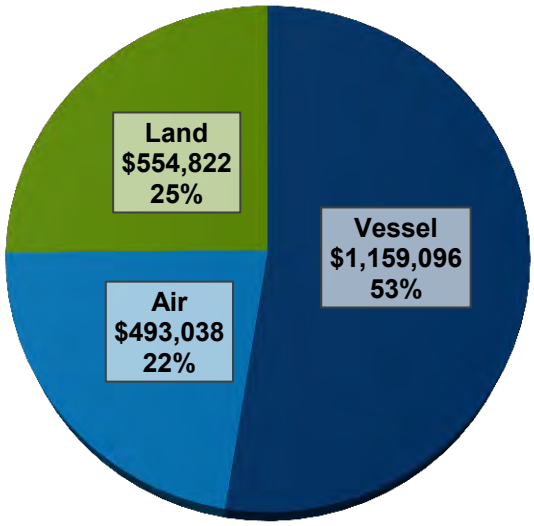
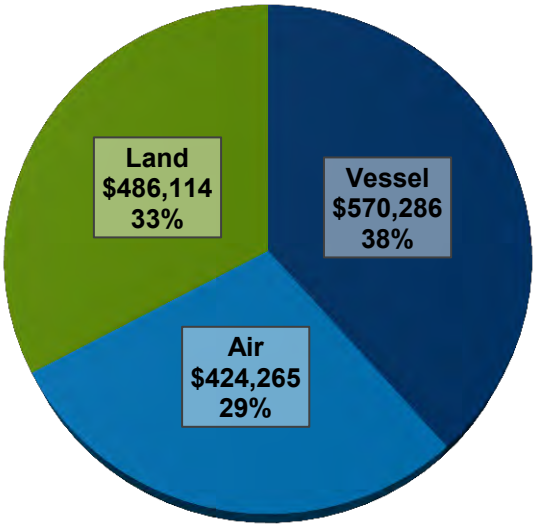


Figure 2: U.S. Export Value by Mode of Transportation, 2011, in Millions of U.S. Dollars



SOURCE Figures 1-2: U.S. Department of Transportation, Bureau of Transportation Statistics, "Maritime Trade and Transportation by the Numbers," accessed December 2013,www.rita.dot.gov/bts/sites/rita.dot.gov.bts/files/publications/by_the_numbers/maritime_trade_and_transportation/index.html

Maritime Mode Overview

- **Maritime is one of seven modes that make up the Transportation Systems Sector.**
- **The Marine Transportation System (MTS) is a geographically and physically complex and diverse system consisting of waterways, ports, and intermodal landside connections that allow the various modes of transportation to move people and goods to, from, and on the water.**
- **The Mode consists of nearly 95,000 miles of coastline, 361 ports, over 25,000 miles of navigable waterways, over 29,000 miles of Marine Highway and 3.4 million square miles of Exclusive Economic Zone.**
- **The Exclusive Economic Zone is the area where the U.S. has jurisdiction over economic and resource management. U.S. Marine Highways are navigable waterways that have been designated by the Secretary of Transportation and have demonstrated the ability to provide additional capacity to relieve congested landside routes serving freight and passenger movement.**
- **Ships plying the maritime domain are the primary mode of transportation for global trade, carrying more than 80 percent of the world's trade by volume.**
- **In addition to the movement of freight, the marine transportation system serves as a critical component of the Nation's passenger transportation network. Over 200 ferry operators provide safe and reliable transportation for passengers and vehicles, while cruise ships and recreational boats contribute billions to the U.S. economy.**
- **The Mode faces current and ongoing risk for Sector facilities and materials due to potential cyberintrusion, port vulnerability, and insecure intermodal shoreside connections.**

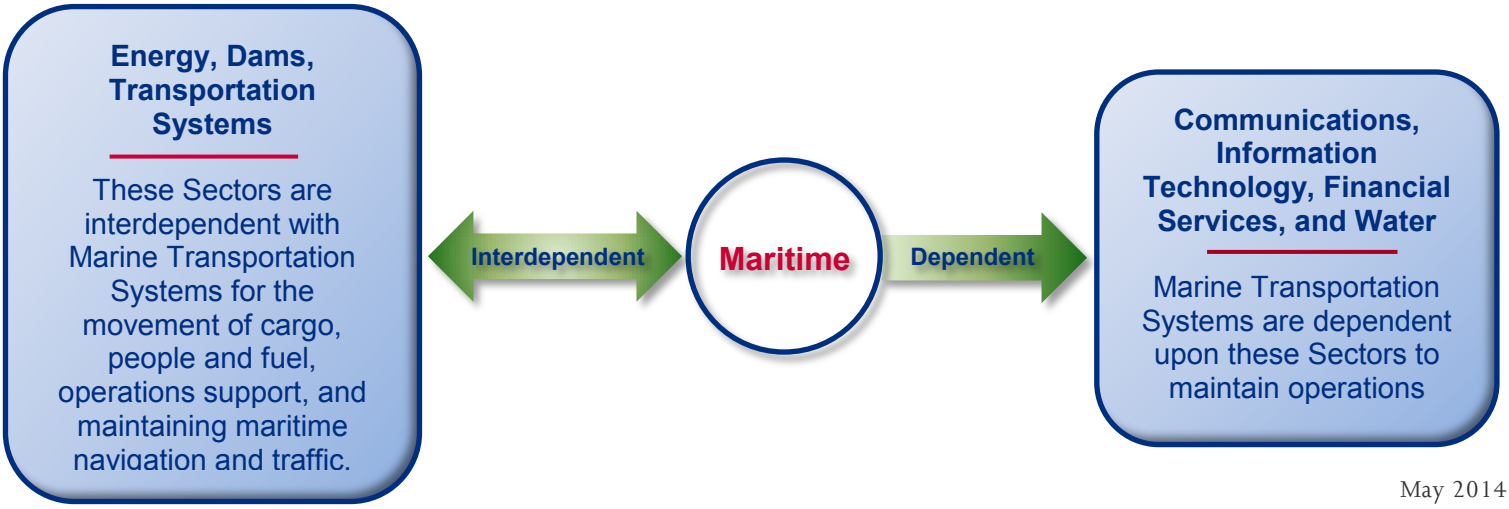
Threats and Hazards of Significant Concern

- **Natural Disasters**
  - From a risk-based perspective, the greatest risk facing the U.S. maritime domain, based on likelihood and consequence, is a major natural disaster, particularly hurricanes, flooding, drought, and tsunami.
  - These events are known to occur frequently and their consequences are often severe.
- **Cybersecurity**
  - Has become more important as the MTS has become increasingly dependent on cybersystems and faces a growing threat from cyberattacks.
  - These systems are used for a variety of purposes, including access control, navigation, traffic monitoring, and information transmission. Although the interconnectivity and utilization of cybersystems facilitate transport, they can also present opportunities for exploitation, contributing to risk for the MTS.
- **Malicious Actors**
  - Even though a robust security planning system (which includes ports, domestic facilities and vessels, as well as foreign vessels that call into the United States) has been implemented through the Maritime Transportation Security Act, a successful attack on critical infrastructure or nodes could cause transportation disruptions with cascading effects.
  - Port facilities and the ships and barges that transit port waterways are also somewhat vulnerable to tampering, theft, and unauthorized persons gaining entry to collect information and commit unlawful or hostile acts. Because of just-in-time method use, a successful attack against one node of maritime infrastructure could disrupt entire systems, cause congestion, limit capacity for product delivery, significantly damage the economy, or create an inability to project military force. Risks related to small vessel security also continue to be a focus of the U.S. Coast Guard (USCG).
- **"Dark Targets"**
  - Numerous maritime security assessments, most notably the DHS Small Vessel Security Strategy and the Current State Report of the Maritime Domain Awareness Interagency Solutions Analysis, have concluded that small "dark targets"—smaller vessels that are not required to carry electronic identification devices, make advance notices of arrival, or otherwise alert authorities to their whereabouts—constitute a major maritime awareness gap.
  - Although the majority of dark targets are legitimate, illicit operators can take advantage of their being difficult to detect and smuggle illegal cargo or people, or serve as waterborne platforms for terrorism.

For More Information

- Sector-Specific Agencies: DHS, Transportation Security Administration (TSA), http://www.tsa.gov, USCG, www.uscg.mil
- U.S. Department of Transportation, Maritime Administration, www.marad.dot.gov
- DHS, *National Risk Profile*, OCIA@hq.dhs.gov
- DHS and TSA, 2010 Transportation Sector-Specific Plan, www.dhs.gov/xlibrary/assets/nipp-ssp-transportation-systems-2010.pdf

Figure 3: Common, First-order Dependencies and Interdependencies of the Maritime Mode



May 2014

Homeland Security

Prepared by the DHS National Protection and Programs Directorate
Office of Cyber and Infrastructure Analysis (OCIA)
Questions or comments should be directed to OCIA@hq.dhs.gov

Homeland Security

Mass Transit Mode
Transportation Sector

Sector Risk Snapshot

Table 1: U.S. Unlinked Passenger Trips by Mode Report Year 2011		
Mode of Service	Passenger Trips	
	Millions	Percent
Bus	5,191	50.3
Bus Rapid Transit	6	0.1
Commuter Bus	37	0.4
Commuter Rail	466	4.5
Demand Response	191	1.9
Ferryboat	80	0.8
Heavy Rail	3,647	35.3
Hybrid Rail	6	0.1
Light Rail	436	4.2
Other Rail Modes*	44	0.4
Publico†	39	0.4
Streetcar	43	0.4
Transit Vanpool	34	0.3
Trolleybus	98	0.9
Total All Modes	10,319	100

*Aerial Tramway, automated guideway transit, cable car, inclined plane, and monorail.
†Publico is a mode of transit service provided by small vans or buses operated in San Juan, PR

Figure 1: Since 2004, Transit Use has Grown More Than Population or Highway Travel

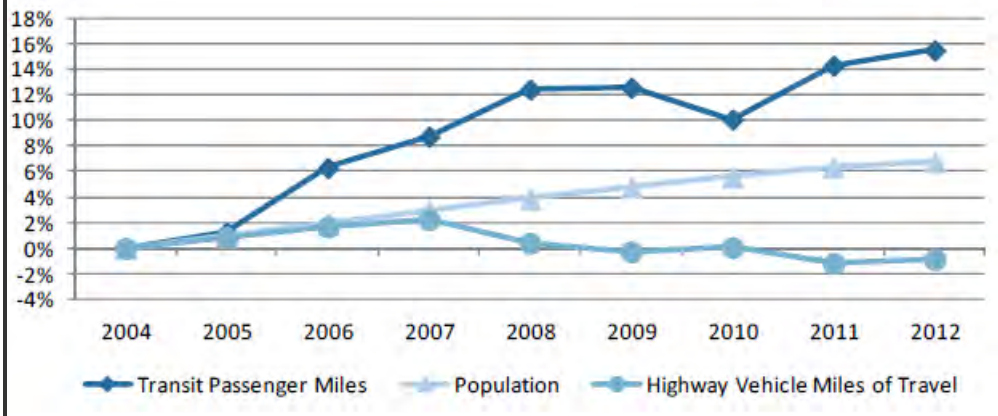


Table 1 and Figure 1 Source: American Public Transportation Association, "2013 Public Transportation Fact Book," Accessed December 2013, www.apta.com/resources/statistics/Pages/transitstats.aspx

Mass Transit Mode Overview

- **The Mass Transit and Passenger Rail Mode includes service by buses, rail transit (commuter rail, heavy rail, also known as subways, and light rail, including trolleys and streetcars), long-distance rail (namely Amtrak and Alaska Railroad), and other, less common types of service. It also includes demand response services for seniors and persons with disabilities, as well as vanpool/rideshare programs and taxi services operated under contract with a public transportation agency. The Mass Transit Mode does not include over-the-road motor coach operators, school bus systems, or private shuttle system operators.**
- **Passengers take 35 million trips each weekday in the United States. As part of an intermodal system of transportation, the Mass Transit Mode also connects to other modes of transportation through multimodal systems and within multimodal infrastructures.**
- **In 2011, U.S. public transportation was provided by 7,100 organizations, ranging from large multimodal systems to single-vehicle special demand response providers.**
- **In 2011, public transportation agencies spent $55 billion for operation of service and capital investment.**
- **The yearly totals for 2011 show that passengers took 10.3 billion trips and rode transit vehicles for 56.1 billion miles.**
- **The Mass Transit Mode includes thousands of employees, operational and maintenance facilities, construction sites, utilities, administrative facilities, and thousands of computerized networks, which facilitate operations and ensure efficient and reliable service.**

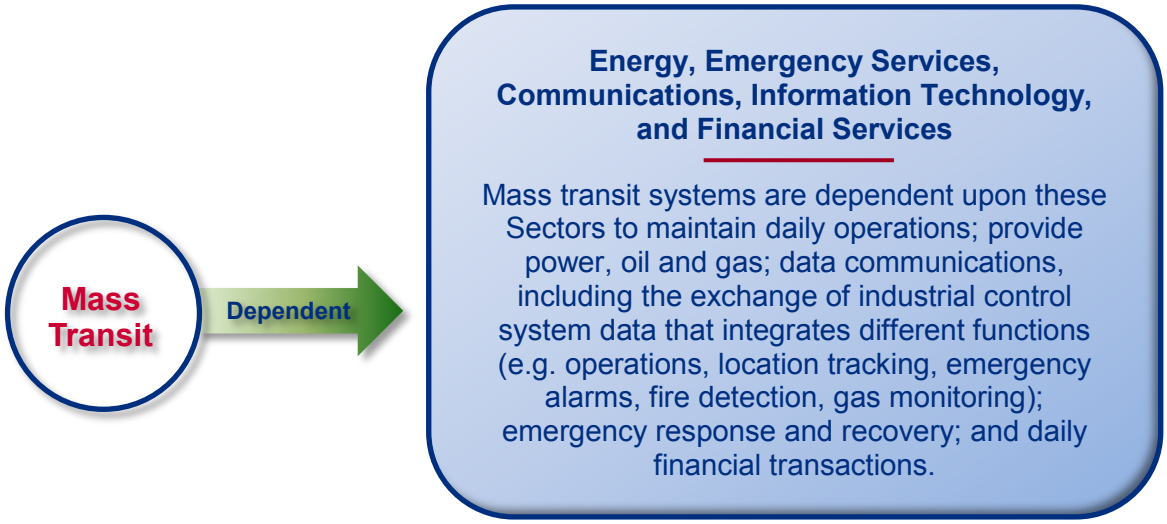
Threats and Hazards of Significant Concern

- **Access**
  - Unlike air transport, where strict access controls and universal security screening apply, public transportation operates more openly, in fast-paced operations with numerous entry, transfer, and exit points, to transport a high volume of passengers every day that greatly exceeds the number of air travelers. Multiple stops and interchanges lead to high passenger turnover, which is difficult to monitor effectively.
  - Broad geographical coverage of mass transit and passenger rail networks provide numerous options for access and getaway and afford the ability to use the system itself as the means to reach the location to conduct the attack.
- **Physical Attacks**
  - Physical attacks on the Mass Transit Mode represents a significant risk to the Sector, and may include a vehicle bomb near a station or track, explosives on a track, release of a caustic or biological agent in an enclosed station, tampering with rail switches, or an improvised explosive device or a lower-yield explosive in a station, train, or bus. Physical attacks on the Mass Transit Mode have to chance to result in scores of casualties. Consequences of such attacks can result in severe economic disruption and can impact the continuity of government operations.
- **Terrorism**
  - Attacks on mass transit systems are an attractive target for terrorists, and can result in a large number of victims, both killed and wounded, significant property damage, and loss of public confidence in public transit systems and Federal, State, local, and tribal governments. Coordinated attacks that simultaneously target multiple nodes in the system can potentially disrupt city-wide public transit operations, increasing public confusion and panic.
  - Examples of coordinated terrorist attacks on the Mass Transit Mode include the 1995 release of sarin gas in the Tokyo subway, which killed 13 people, severely injured 50, and caused temporary vision problems in over a 1000 others, and the 2005 bombings in London, in which IEDs were detonated in three London Underground trains across the city and a double-decker bus. The London bombings resulted in the deaths of 52 civilians and over 700 casualties.

For More Information

- Sector-Specific Agencies: DHS, Transportation Security Administration (TSA), www.tsa.gov and Department of Transportation, www.dot.gov
- American Public Transportation Association, www.apta.com
- DHS, *National Risk Profile,* OCIA@hq.dhs.gov
- DHS and TSA, *2010 Transportation Sector-Specific Plan*, www.dhs.gov/xlibrary/assets/nipp-ssp-transportation-systems-2010.pdf

Figure 2: Common, First-order Dependencies of the Mass Transit Mode



May 2014

Homeland Security

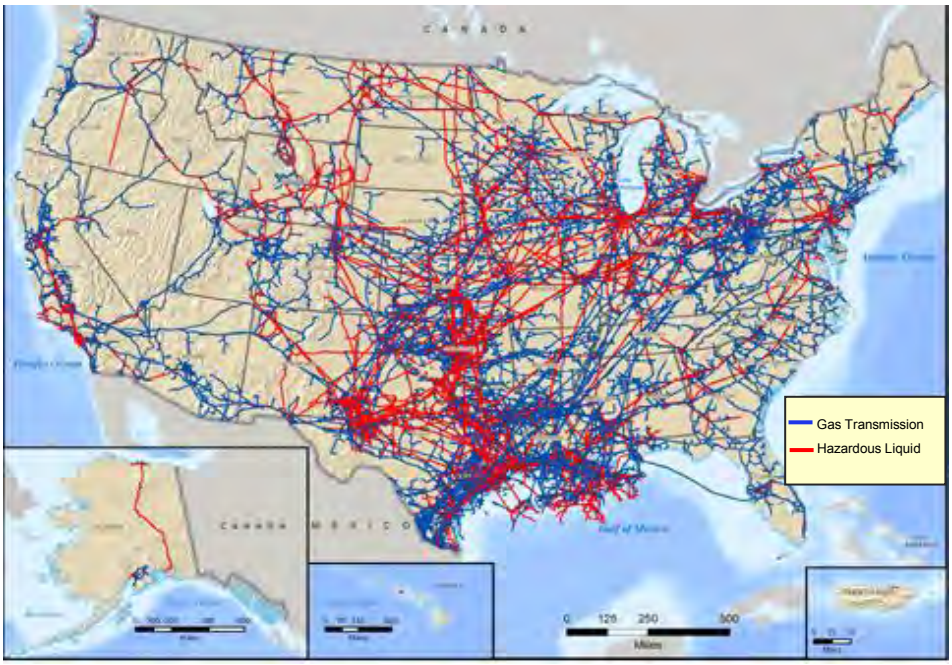
Prepared by the DHS National Protection and Programs Directorate
Office of Cyber and Infrastructure Analysis (OCIA)
Questions or comments should be directed to OCIA@hq.dhs.gov

Homeland Security

Pipeline Mode
Transportation Sector

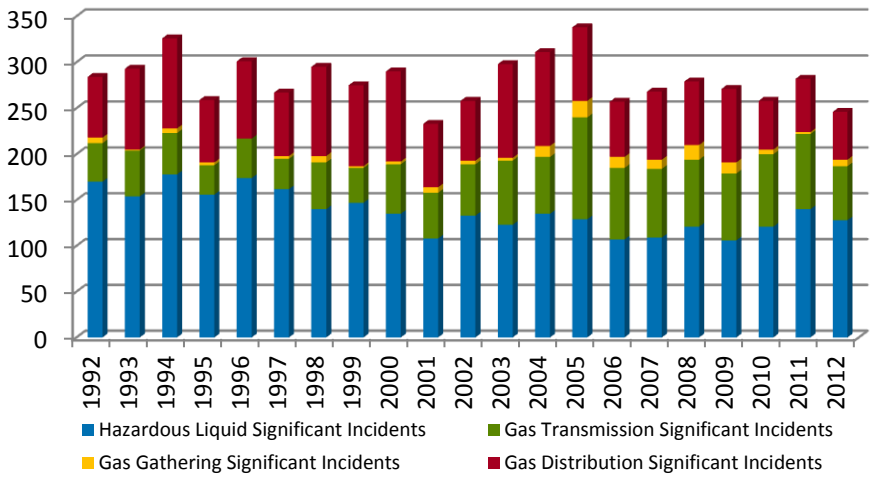
Sector Risk Snapshot

Figure 1: U.S. Gas Transmission and Hazardous Liquid Pipelines



Source: U.S. Department of Transportation, Pipeline and Hazardous Materials Safety Administration (PHMSA), National Pipeline Mapping System, March 2012.

Figure 2: Number of Significant Pipeline Systems Incidents 1992-2012*



*Significant Incidents are those incidents reported by pipeline operators when any of the following specifically defined consequences occur: 1) fatality or injury requiring in-patient hospitalization; (2) $50,000 or more in total costs; (3) highly volatile liquid releases of 5 barrels or more; or, (4) other liquid releases of 50 barrels or more resulting in an unintentional fire or explosion.

Source: PHMSA, *Significant Pipeline Incidents*, http://primis.phmsa.dot.gov/comm/reports/safety/sigpsi.html

Pipeline Mode Overview

- Pipelines are one of seven modes that make up the Transportation Sector.
- More than 2.5 million miles of pipelines network the United States to transport nearly all of the natural gas and about 65 percent of hazardous liquids, including crude and refined petroleum products, consumed within the United States.
- There are four main types of pipelines, most of which are buried underground: 1) Natural Gas Transmission and Storage; 2) Hazardous Liquid Pipelines and Tanks; 3) Natural Gas Distribution; and 4) Liquefied Natural Gas (LNG) Processing and Storage Facilities.
- Cross-border (international) pipelines are becoming increasingly important to the Nation's pipeline industry, which is prompting the U.S. and Canada to conduct joint assessments on trans-border infrastructure and identify necessary additional protective measures.
- While most pipelines are buried, the system has above-ground assets (e.g. wellheads, compressor stations, pumping stations, and processing facilities) that may be vulnerable to attack.
- The Mode faces current and ongoing risk to the movement of pipeline materials via direct attack upon critical pipeline system infrastructure and from cyberattacks against pipeline control systems and networks.

Toxic Inhalation Hazard

- A successful deliberate terrorist attack against toxic inhalation hazard (TIH) materials poses serious risks of fatalities and injuries, especially if the attack were to occur in a highly populated urban area.
- Pipelines are used to transport TIH chemicals such as anhydrous ammonia, a critical fertilizer for the American farming industry and feedstock for the chemical industry.

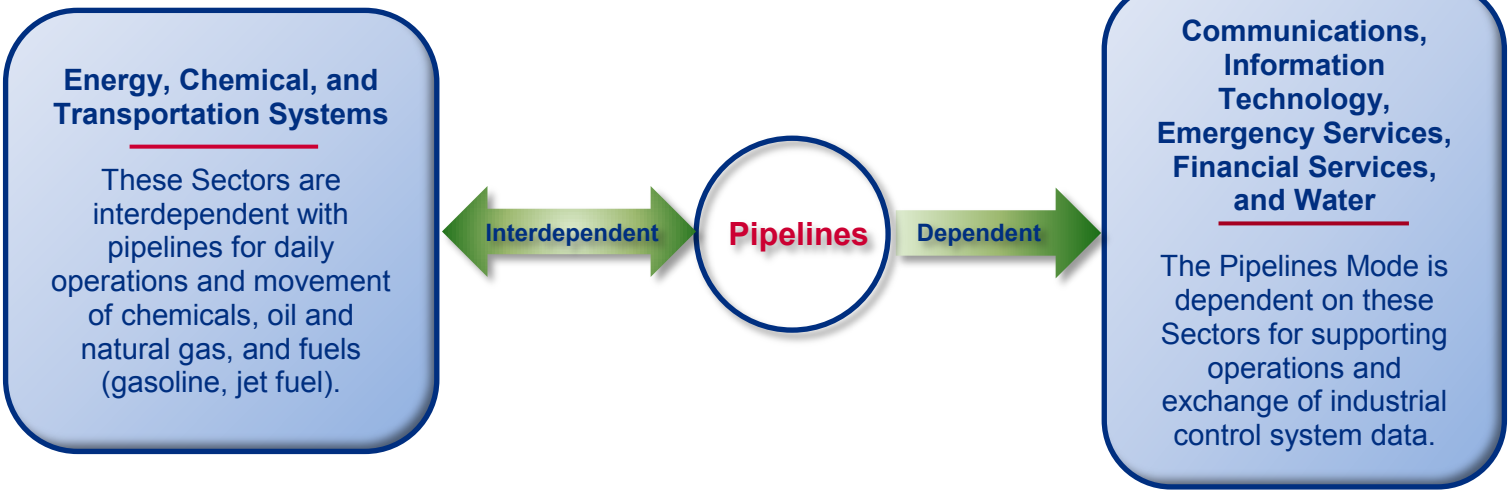
Threats and Hazards of Significant Concern

- **Release of Pipeline Materials**
  - The pipeline system is uniquely vulnerable to terrorist attacks because of the products transported and because pipeline networks are widely dispersed across both remote and urban portions of the country.
  - Many pipelines carry volatile and flammable materials that have the potential to cause serious injury to the public and the environment. A pipeline facility could be vandalized or attacked with explosive devices, resulting in flow disruption or the release of its contents.
- **Cyberthreats**
  - Pipelines are also susceptible to cyberattacks on their computer control systems. Cyberthreats could result from the acts of a terrorist-hacker or a rogue employee with computer access.
  - The latter threat requires that specific attention be given to personnel security credentials and access protocols, as well as general cybersecurity protocols.
- **Cascading Effects from Disruptions to Critical Dependencies**
  - In addition, attacks on other infrastructure, such as regional electricity grids and communication networks, could cause a serious disruption in pipeline operations, posing risks for all Sectors serviced by pipelines, including the military and major commercial installations (Figure 3).

For More Information

- Sector-Specific Agencies: DHS, Transportation Security Administration (TSA), www.tsa.gov, Department of Transportation, www.dot.gov
- Pipeline and Hazardous Materials Safety Administration (PHMSA), www.phmsa.dot.gov
- American Petroleum Institute, www.api.org
- American Gas Association, www.aga.org
- DHS, *National Risk Profile*, OCIA@hq.dhs.gov
- DHS and TSA, *2010 Transportation Sector-Specific Plan*, www.dhs.gov/xlibrary/assets/nipp-ssp-transportation-systems-2010.pdf
- Interstate Natural Gas Association of America (INGAA) , www.ingaa.org
- Association of Oil Pipelines (AOPL), www.aopl.org

Figure 3: Common, First-order Dependencies and Interdependencies of the Pipeline Mode



May 2014

Homeland Security

Prepared by the DHS National Protection and Programs Directorate
Office of Cyber and Infrastructure Analysis (OCIA)
Questions or comments should be directed to OCIA@hq.dhs.gov

Homeland Security

Postal and Shipping Mode
Transportation Sector

Sector Risk Snapshot

Table 1: Size of the U.S. Mailing Industry

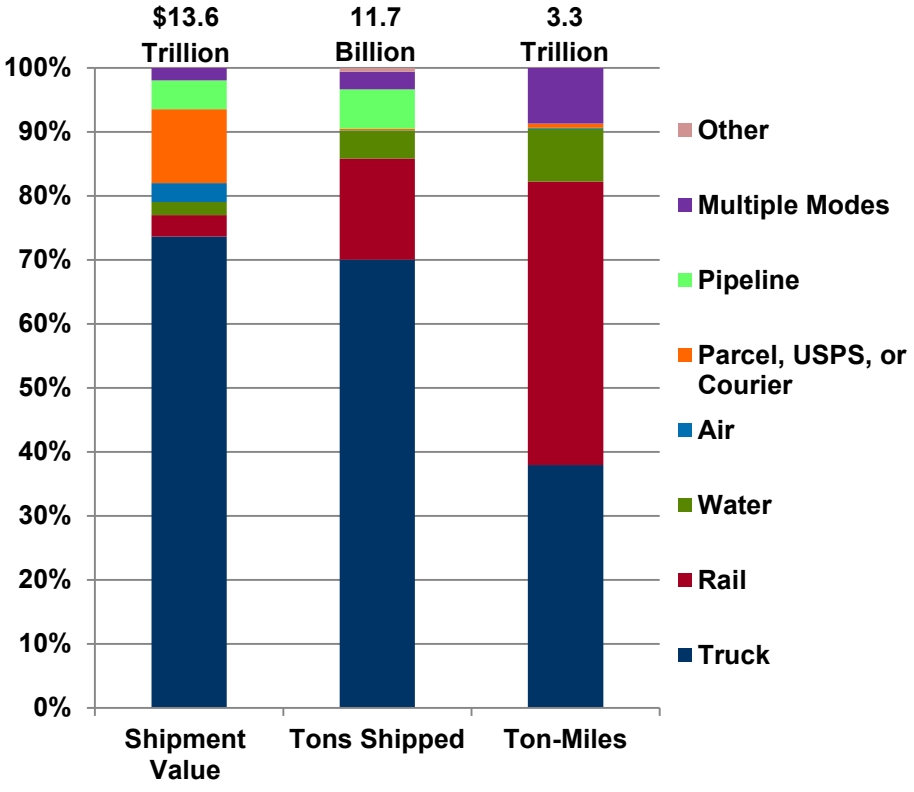
The size of the mailing industry compared to other key U.S. industries is significant. What happens in the mailing industry echoes throughout the economy as it supports over 8.6 percent of the U.S. Gross Domestic Product.

Industry	Number of Jobs Supported	Annual Revenue Supported
Mailing	8.4 million	$1.3 Trillion
Airline	10.0 Million	$1.0 Trillion
Oil and Natural Gas	9.6 million	$1.1 Trillion

SOURCE: U.S. Postal Service, *USPS FY2013 Annual Report to Congress*, 2013.

Figure 1: Value, Tonnage, and Ton-Miles of Shipments by Mode

In 2012, parcel delivery, USPS, and other courier services accounted for 11.6 percent of shipments by value, but less than half of one percent by tonnage, demonstrating that the Postal and Shipping industry typically ships higher value products.



SOURCE: U.S. Department of Transportation, Bureau of Transportation Statistics and U.S. Department of Commerce, U.S. Census Bureau, *2012 Economic Census: Transportation Commodity Flow Survey*, Preliminary Release, December 2013.

Postal and Shipping Mode Overview

- Postal and Shipping is one of seven modes that make up the Transportation Sector.
- Postal and Shipping was formerly recognized as a stand-alone Sector until the February 2013 release of Presidential Policy Directive-21 (PPD-21), when Postal and Shipping was incorporated into the Transportation Sector.
- Composed of large integrated carriers, regional and local courier service providers, mail services and mail management firms, and chartered air delivery services.
- Four large integrated carriers—the U.S. Postal Service (USPS), the United Parcel Service (UPS), FedEx, and DHL International—account for 94 percent of the Mode's assets systems, networks, and functions.
- Postal and Shipping moves more than 720 million messages, products, and financial transactions each day.
- The threat environment to the mode includes attacks on infrastructure, operations, and employees, and the use of the Mode to attack its customers, other Sectors, or the economy as a whole, using targeted or widespread techniques and tactics.
- Mode risk is a function of the vulnerability of an extremely large number of collection points, many of which are open and anonymous.
- The Mode is a highly trusted entity, and its employees and representatives have ready access to businesses and residences throughout the country.
- The Mode faces current and ongoing risk, due to terrorist attacks using hazardous materials, as well as chemical, biological, radiological, and nuclear explosives (CBRNE) for mail-based attacks.

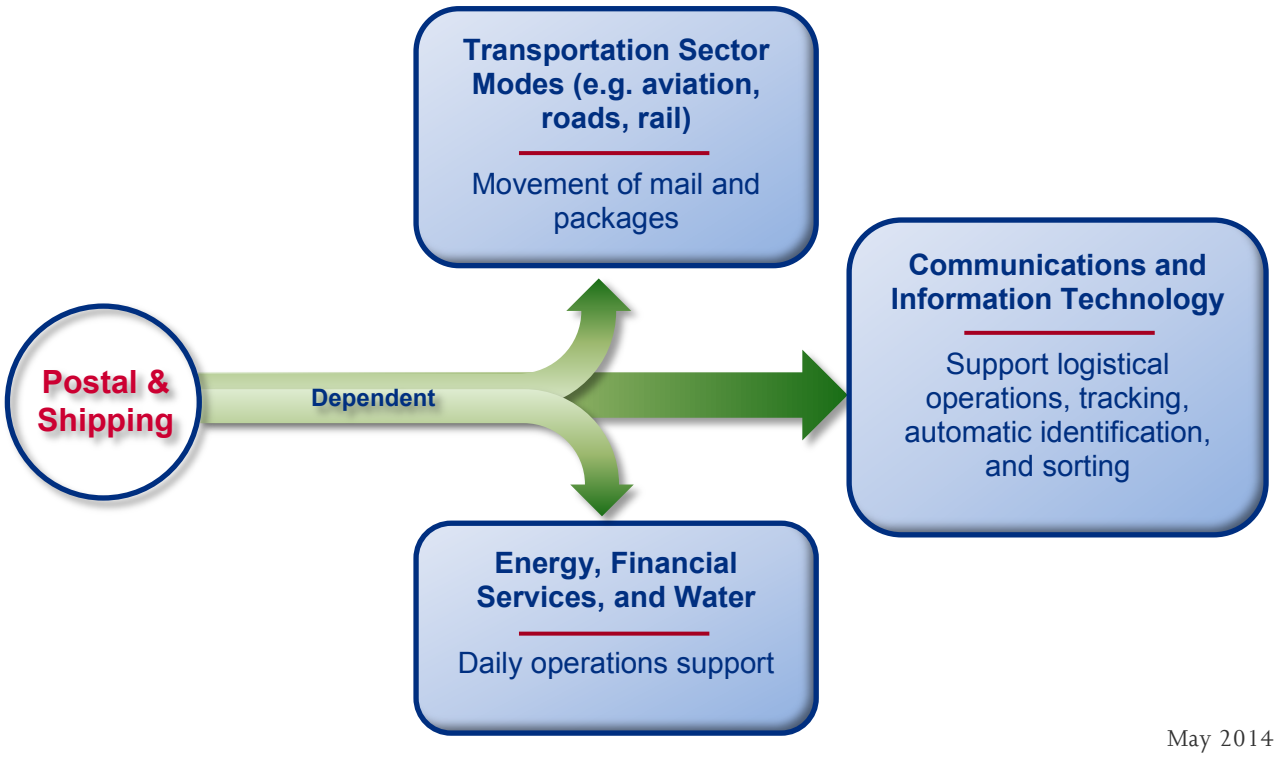
Threats and Hazards of Significant Concern

- **Open Access and Entry Points**
  - By design, the Postal and Shipping Mode is an open system with an extremely large number of entry and collection points, many of which are anonymous. These facilities present a vast number of entry points where dangerous materials could be inserted for delivery to intended targets.
- **Mail-based Threats**
  - Mail-based threats pose a significant and continuing risk for the Postal and Shipping Mode. For example, the Unabomber, Ted Kaczynski, hand-delivered or used the Postal Service over the course of 17 years to deliver parcel bombs that killed three Americans and injured 24 more (FBI, 2008).
  - Physical attacks using improvised explosive devices (letter bombs and parcel-based attacks) against postal and shipping facilities, or against other Sectors, could result in changes in the flow of ground and air mail and delays in mail service.
  - Postal and shipping infrastructure may be severely disrupted by such attacks, which may further complicate an overall disaster emergency response due to multiple cross-sector interdependencies (Figure 2).
- **Attacks Using Hazardous Materials or CBRNE**
  - The Postal and Shipping Mode is one of the few infrastructures that have been threatened by biological agents; in 2001, the USPS was used as a vehicle for delivering anthrax against multiple targets.
  - In 2010, the terrorist organization Al-Qaeda in the Arabian Peninsula (AQAP) planted bombs in two packages of printer cartridges found on separate cargo planes. Both U.S. and U.K. intelligence officials speculated that the bombs were probably designed to detonate mid-air, with the intention of destroying both planes over Chicago or another city in the U.S. (BBC, 2010, www.bbc.co.uk/news/world-us-canada-11671377)

For More Information

- Sector-Specific Agencies: DHS, Transportation Security Administration (TSA), www.tsa.gov, Department of Transportation, www.dot.gov
- USPS, www.usps.com and http://about.usps.com/securing-the-mail/mail-security-center.htm
- DHS, *National Risk Profile,* OCIA@hq.dhs.gov

Figure 2: Common, First-order Dependencies of the Postal and Shipping Mode



May 2014

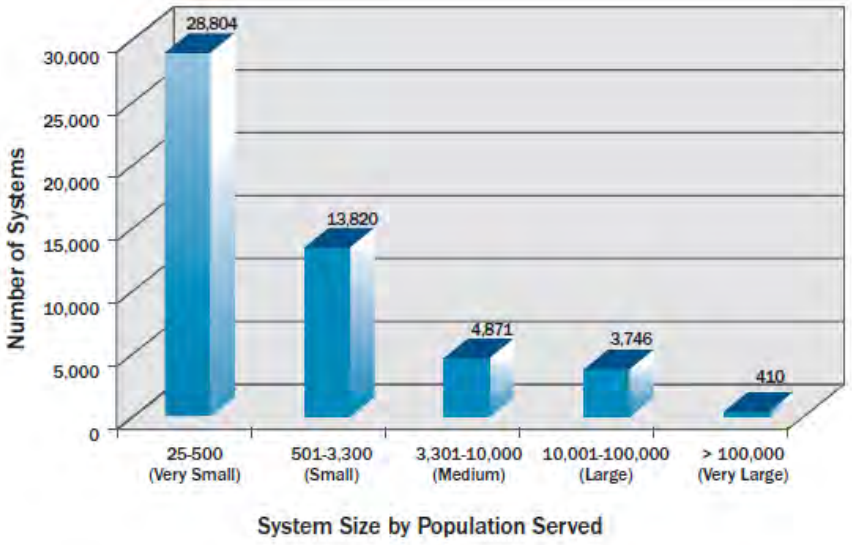
Homeland Security

Prepared by the DHS National Protection and Programs Directorate
Office of Cyber and Infrastructure Analysis (OCIA)
Questions or comments should be directed to OCIA@hq.dhs.gov

Homeland Security

Water and Wastewater Systems Sector
Sector Risk Snapshot

Figure 1: Community Drinking Water Systems and System Size.
Source: EPA, Safe Drinking Water Information System (SDWIS)



Drinking Water

- A drinking water contamination incident or the denial of drinking water services would have far-reaching public health, economic, environmental, and psychological impacts across the Nation.
- Other critical services, such as fire protection, healthcare, and heating and cooling processes, would also be disrupted by the interruption or cessation of drinking water service, resulting in significant consequences to the national or regional economies.
- The majority of community water systems (CWS) are small systems that serve approximately 8 percent of the population who get their water from CWS (Figure 1).
- Only 17 percent of CWS are classified as medium or large systems, but these systems serve the majority of the U.S. population.
- The EPA reports that CWS served 300.2 million people, while non-community water systems (e.g. schools, factories, hospitals, campgrounds, and gas stations that have their own water systems) served 19.5 million people in 2010.

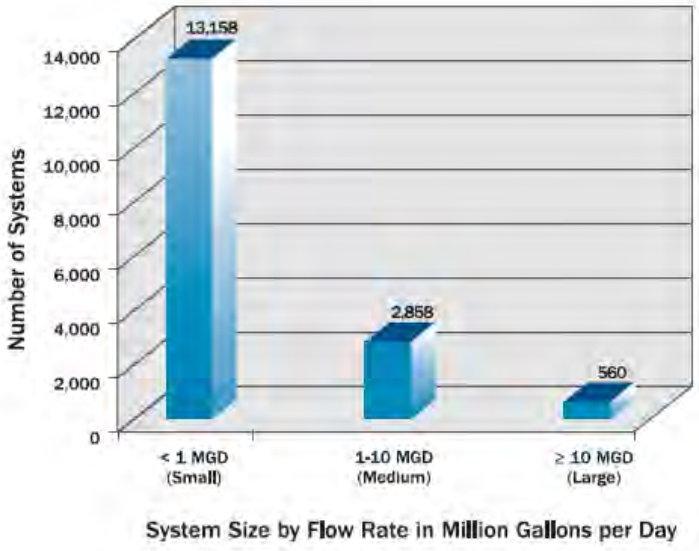
Wastewater

- Disruption of a wastewater treatment utility or service can cause loss of life, economic impacts, and severe public health and environmental impacts.
- If wastewater infrastructure were to be damaged, the lack of redundancy in the Sector might cause denial of service to domestic and industrial users.
- The majority of utilities are small in size, and provide wastewater treatment to approximately 23 million people (Figure 2).
- The medium or large size utilities systems serve the majority, at about 90 percent of the population.

Water Sector Overview

- **Comprises approximately 155,000 public drinking water systems (includes both community and non-community water systems, such as schools, factories and campgrounds) and approximately 16,500 publicly owned wastewater treatment utilities (EPA, 2012 and DHS, 2010).**
- **Water utilities consist of source waters, treatment facilities, pumping stations, storage sites, and extensive distribution, collection, and monitoring systems.**
- **The Water Sector is vulnerable to a variety of all-hazard threats including contamination with deadly agents; insider threats; physical attacks using improvised explosive devices (IEDs); cyberattacks; and natural hazards.**
- **Successful attacks on a drinking water or wastewater system could result in large numbers of illness, casualties, and denial of service, which could severely impact the Nation's public health and economic vitality.**

Figure 2: Publicly Owned Wastewater Treatment Works and System Size



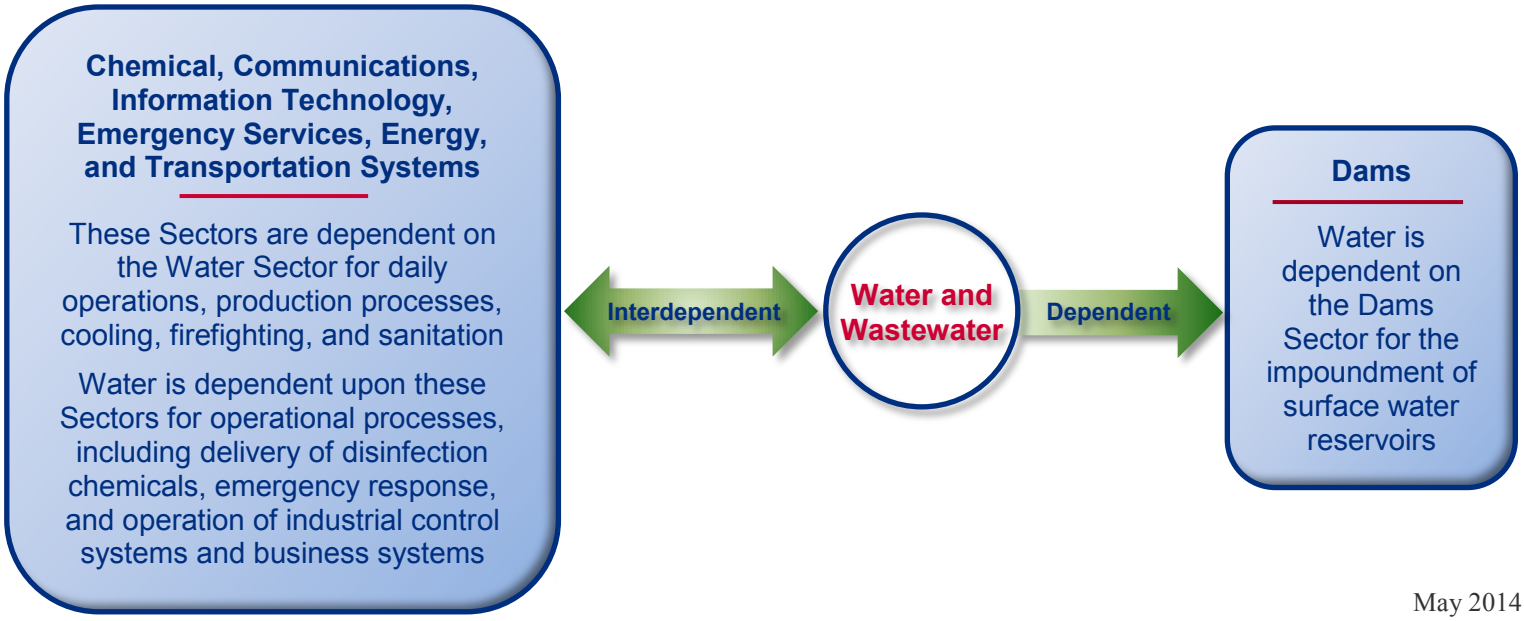
Threats and Hazards of Significant Concern

- **Chemical, Biological, or Radiological Contamination**
  - Most public water supplies are monitored and treated to prevent the distribution of contaminated drinking water.
  - The risk of CBR contamination stems from both the enduring terrorist threat to contaminate the U.S. water supply and the serious health impacts that could result from an undetected contaminant.
  - These impacts could vary depending on the type of substance, route of exposure (ingestion, absorption, inhalation), and amount of time before the contaminant is detected.
- **Natural Hazards**
  - Natural hazards, such as hurricanes, tornadoes, floods, earthquakes, and drought, pose a serious and continuing risk for the Sector.
  - Water infrastructure may be severely disrupted or destroyed by such hazards, which may further complicate an overall disaster emergency response due to multiple cross-sector interdependencies (Figure 3).
  - Critical water shortages may also result from drought conditions and climate change, leading to water use restrictions and rationing.
- **Physical and Cyberattacks by Terrorists, Homegrown Extremists, or Disgruntled Insiders**
  - Physical attacks using IEDs on chemical storage tanks or other critical nodes in a drinking water or wastewater system could result in a release of hazardous materials or in a long-term loss of service should a "single-point-of-failure" be destroyed.
  - Cyberattacks and intrusions on supervisory control and data acquisition (SCADA) systems or other business systems pose a serious threat to the Water Sector, allowing malicious actors to manipulate or exploit control systems essential to operation of drinking water and wastewater utilities.

For More Information

- Sector-Specific Agency: Environmental Protection Agency, www.epa.gov/
- Environmental Protection Agency (EPA), Water Security, http://water.epa.gov/infrastructure/
- DHS, *Infrastructure Protection Report Series: Community Water Systems (CVPIPM)*, version: 29 August 2011
- DHS and EPA, *2010 Water Sector-Specific Plan*, hwww.dhs.gov/files/programs/gc_1179866197607.shtm
- DHS, *National Risk Profile,* OCIA@hq.dhs.gov

Figure 3: Common, First-order Dependencies and Interdependencies of the Water Sector



May 2014

Homeland Security

Prepared by the DHS National Protection and Programs Directorate
Office of Cyber and Infrastructure Analysis (OCIA)
Questions or comments should be directed to OCIA@hq.dhs.gov

The Office of Cyber and Infrastructure Analysis (OCIA) produces Sector Risk Snapshots in support of the Homeland Security Enterprise as part of the Department's efforts to carry out comprehensive assessments of the risks to critical infrastructure, and to facilitate a greater understanding of the emerging threats to and vulnerabilities of critical infrastructure in the United States. For more information, contact OCIA@hq.dhs.gov or visit our Website at www.dhs.gov/office-cyber-infrastructure-analysis.

Homeland
Security

IECC Cyber Vulnerabilities Whitepaper

Communications Sector

January 2018

LTC David L. Skalon
2 January 2018

BACKGROUND:

Reliance upon an interconnected backbone as an enabler to other sectors has evolved from convenience to necessity. "Over the last 25 years, the (telecommunications) sector has evolved from predominantly a provider of voice services into a diverse, competitive, and interconnected industry using terrestrial, satellite, and wireless transmission systems."[1] With this reliance comes the burden of securing transmissions while meeting the growing need for bandwidth. When considering the playing field for this sector, like many other Indiana sectors, it is a divide between the larger corporations and the smaller, mom and pop providers.

The appetite for connectivity has grown exponentially and reaches down to children of a decreasing age every year. Today's generation does not know of a time without the internet and demands its availability and reliability. Providing that backbone has necessitated the moves to the various platforms and systems listed previously. This reliance makes it a desirable target for emotional and financial impact, but where does the risk really exist?

GOVERNANCE, REGULATORY AND SUPPORT ASSOCIATIONS:

- U.S. Department of Homeland Security (DHS) - Designated as the lead agency for the Communications Sector at the national level.
- Indiana Utility Regulatory Commission (IURC)- Monitors and evaluates regulatory proceedings and policy initiatives at the federal, state, and local levels that affect telephone, cable, and internet service providers in the state.
- Federal Communications Commission (FCC)- Regulates interstate and international communications by radio, television, wire, satellite, and cable in all 50 states, the District of Columbia and U.S. territories.
- Indiana Exchange Carrier Association (INECA)- Advocates for its member companies on federal and state issues, to educate government leaders as well as the public at large on the importance of modern telecommunications to rural communities.
- Indiana Broadband Telecommunications Association (IBTA)- Trade association representing Indiana's Broadband and Technology industry.
- National Exchange Carrier Association (NECA)- Supports local telecommunications companies. We are dedicated to helping our members provide broadband-based solutions to keep their customers connected.
- National Rural Telecommunications Cooperative Association (NRTC)- Provides solutions that help our electric and telephone members bring all of the advantages of today's evolving technology to rural America.

[1] DHS, https://www.dhs.gov/communications-sector, details the national perspective of this sector, retrieved February, 2018.

- National Telecommunications and Information Administration (NTIA)- Executive Branch agency that is principally responsible for advising the President on telecommunications and information policy issues.
- National Telecommunications Cooperative (NTCA)- The Rural Broadband Association is the premier association representing nearly 850 independent, community-based telecommunications companies that are leading innovation in rural and small-town America.
- North American Numbering Plan Administration (NANPA)
- United States Telecom Association (USTA)

RISKS:

The infrastructure is vast and diverse, many different types of risks could compound to make widespread outages possible. The risks span from basic outages to 2nd and 3rd order effects that could put many people in harm's way as depicted below:

1. Natural disasters and extreme weather have increased in frequency and severity over the past few years with varying levels of impact to our communication infrastructure. In Indiana, the most likely threats are floods, snow storms, and tornados. Solar flares from the sun also pose a less frequent, but potential threat as well.
2. The Communications Sector depends on suppliers for the products and services that are necessary to deliver communication services to users. In particular, the sector is dependent on reliable hardware and software. This is an area the sector continues to scrutinize closely.
3. Cyber threats include the typical software and hardware exploits that impede the end user's devices, but these attacks can have a cascading impact on the infrastructure it operates on.
4. Larger providers have the staff and processes to prevent and mitigate known risks and train their personnel on best practices. Smaller providers do not have the capital or expertise to prevent or react at the same level as the larger providers.

PAST ATTACKS:

Although the media is now starting to cover cyber attacks at an increased rate, it is still not real to the average consumer, unless they have experienced and outage or inconvenience. Attacks like the one in a region of California from 2015 details the impact that physical attacks have on infrastructure:

Someone continues to target critical communications infrastructure in a region of the U.S., on Monday, September 14, unknown attackers cut backbone fiber optic Internet cables in Livermore California. This is not an isolated attack, law enforcement counted fourteenth attacks on critical communications infrastructure in the same region and security experts suspect that the attackers are carrying out the sabotage for economic and cyber warfare.

The investigation on such kind of attacks is conducted by the FBI because AT&T's fiber optic network is considered to be part of the nation's critical communication infrastructure.

"Someone deliberately severed two AT&T fiber optic cables in the Livermore, Calif., Monday night, the latest in a string of attacks against the Internet's privately run backbone*." reported the USA Today website.*

SECTOR SPECIFICS:

The communications sector has several subsections to it: telephone companies, wireless providers, Internet and Voice over Internet Protocol (VOIP) providers, and Cable/Internet providers. Indiana has been known to have a lot of small or 'mom and pop' utilities and the telecommunications sector is no different. However, based on scope and impact to the national infrastructure, some nodes within the state have a higher risk associated with them. Some of these are run as cooperatives or by local municipal/city councils, etc; it varies by location.

BOTTOM LINE:

In light of the challenges stated above; aging infrastructure, competition between repairing infrastructure vs improving cyber security and the clear lack of governance as it relates to cyber security leave this sector somewhat vulnerable to attack as compared to other critical infrastructure sectors. The level of risk is based on scale. Larger providers have robust architecture, security processes and protocols to minimize impact. Smaller providers is where the higher risk is found. The recommended approach to these elements is outreach and education to initiate the actions to protect. The awareness factor alone can prevent the lower echelon threats while improving the overall health of our telecommunication services.

IECC Cyber Vulnerabilities Whitepaper

Energy Sector

February 2018

GOVERNOR ERIC J. HOLCOMB'S
INDIANA EXECUTIVE COUNCIL ON CYBERSECURITY

Cyber Vulnerabilities Whitepaper - Energy Sector

Carl A Cahill
Walter Grudzinsk
Stan Partlow Jr.
27 February 2018

BACKGROUND:

The Energy Sector powers the lives and businesses of Indiana residents. Computers, traffic lights, water pumps, furnaces, air conditioners, ATMs, stoves, refrigerators, and many other devices require electricity. Innovation continues to drive new uses for electricity by integrating computers with day-to-day devices as the Internet of Things (IoT) rapidly expands.

Power is the foundational component of modern society. Presidential Policy Directive 21 states the Energy Sector is "uniquely critical" as it enables all other critical sectors.[1] The Energy Sector is classified as Critical Infrastructure and is heavily regulated to ensure the reliability of power to residents and businesses.

Cybersecurity is a key topic in the Energy Sector due to the potential impacts disruption of power could have to society. Cyber threat actors have shown an increased interest in having capabilities to disrupt the generation and distribution of power.[2] The Energy Sector remains focused on providing reliable power through resilient and defensible systems.

GOVERNANCE, REGULATORY AND SUPPORT AGENCIES:

- Federal Energy Regulatory Commission (FERC) – is an independent agency that regulates the interstate transmission of electricity, natural gas, and oil. FERC has additional powers and responsibilities outlined in The Energy Policy Act of 2005.[3] https://www.ferc.gov/
- Indiana Utility Regulatory Commission (IURC) – Energy Division Regulates pricing models and quality of service but stops short of mandating cyber defense standards. https://www.in.gov/iurc/2340.htm
- North American Electric Reliability Corporation (NERC) – is an international not-for-profit regulatory authority responsible for assuring reliability and security of the bulk power system in North America. NERC is responsible for publishing Critical Infrastructure Protection (CIP) physical and cybersecurity requirements to protect bulk electric systems. http://www.nerc.com/Pages/default.aspx
- ReliabilityFirst Corporation (RFC) – is the regional organization, approved by FERC, responsible for the reliability of the North American Bulk-Power system in Indiana. https://www.rfirst.org/
- Department of Energy (DOE) – federal agency tasked with advancing the Energy Sector and enabling reliable and resilient energy at the federal level. https://energy.gov/
- Federal Bureau of Investigations – is the government agency responsible for investigating cyber-crime. https://www.fbi.gov/
- Department of Homeland Security (DHS) – is the government agency responsible for assisting critical infrastructure with combating cyber-crime. https://www.dhs.gov/

[1] https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil
[2] https://www.energy.senate.gov/public/index.cfm/files/serve?File_id=5F40E0A2-B836-40EA-ACC6-9BF3B43A1B8F
[3] https://www.ferc.gov/about/ferc-does.asp

RISKS:

Impacts of a successful cyber-attack on a utility company vary greatly depending on the motivation of the threat actor, the depth of the infiltration, and the sophistication of the utility's defenses. The two highest risk scenarios are:

1) The disruption of the generation and distribution of power.
2) The loss of Customer personally identifiable information (PII)

Impacts and likelihood of a cyber event resulting in the disruption of the generation and distribution of power continue to be a point of debate within the Nation. The threat actors capable of performing this type of attack consist primarily of Nation States. Nations States are unlikely to attack the grid due to the threat of military action. The impacts of such an event will depend on the duration of power disruption and the scale of population affected. Loss of power for a few hours will result in some economic loss. Longer term, large scale power loss can lead to society breakdowns as basic necessities such as food, water, and livable shelter become scarce. 2016 marked the development and use of the first ever malware framework built specifically to attack the power grid.[4] Malware such as Crashoverdrive demonstrate threat actors are motivated to have capabilities to disrupt power.

Theft of Customer PII is likely performed by a different threat actor than those looking to attack the power grid. Cyber criminals are motivated to steal PII for financial gain. Energy companies keep social security numbers for Customers and in some cases credit card and bank account information. All three data types are highly desirable for financially motived threat actors. Energy Companies have different methods for preventing the loss of Customer PII including the use of encryption, least privilege, and network segmentation.

PAST ATTACKS:

A significant increase in Industrial Control System (ICS) based cyber activity highlighted 2016 and 2017 for the Energy Industry. Five unique ICS threat actors were active and two ICS specific malware variants were discovered.[5] Also disruptive IT malware, such as WannaCry, became a potential concern for the Energy Industry.

The Energy Industry has experienced a small number of successful targeted attacks over the last 10 years. Most of the threat actors targeting the disruption of the power grid are Nation States. Nation States are less likely to execute an attack and more likely to stage malware for future attacks if needed in a time of war or to make a political statement.[6]

Stuxnet – In June of 2010 the first cyber-attack on the Energy Industry took place on an Iranian nuclear power plant. The United States and Israeli governments are suspected to have developed and executed this cyber-attack.

Ukraine – in 2015 and 2016 the Ukraine experienced power outages due to cyber-attacks. A framework specific to the Energy Industry was used in the 2016 cyber-attack. The threat actor Electrum, with ties to

[4] https://dragos.com/blog/crashoverride/CrashOverride-01.pdf
[5] https://www.energy.senate.gov/public/index.cfm/files/serve?File_id=5F40E0A2-B836-40EA-ACC6-9BF3B43A1B8F
[6] https://www.csoonline.com/article/3260624/critical-infrastructure/insecure-by-design-what-you-need-to-know-about-defending-critical-infrastructure.html

Sandworm, was responsible for the 2016 Ukraine attack. The CRASHOVERRIDE, an ICS specific malware framework, was developed and used in this attack.

Nuclear 17 / Palmetto Fusion – In 2017 Energy companies in the United States were targeted by threat actors. A nuclear power plant in Kansas had non-Nuclear controls systems compromised.[7] This cyber-attack started with a phishing campaign. Russia-based threat actors are suspected in this targeted attack.

UK / Ireland – Russia-based threat actors target the UK and Irish power grid in a series of cyber-attacks in 2017. Power was not disrupted. Investigators suspect Russia was attempting to put malware on systems to use at a later date to potentially disrupt the grid and cause power outages.[8]

SECTOR SPECIFICS:

The Energy Sector is regulated and partners closely with government agencies. Relationships with both regulators and government agencies has helped advanced and formalize some cyber capabilities for the industry.

FERC and NERC provide oversight for cybersecurity controls to support reliability requirements for the Bulk-Electric Systems. NERC has issued prescriptive controls known as Critical Infrastructure Protection (CIP) which are audited and enforced.

The Department of Homeland Security (DHS), Department of Energy (DOE), and Federal Bureau of Investigations (FBI) continue to develop programs such as Enhanced Cybersecurity Services (ECS), Cybersecurity Risk Information Sharing (CRISP), and Electricity Sector Information Sharing and Analysis Center (E-ISAC). These programs help participating utilities detected and protect against advanced cyber threats through analysis and information sharing.

The Energy Sector has a unique program called Cyber Mutual Assistance (CMA). CMA is an agreement between participating utilities to provide support during a cyber event. Support might include sending cybersecurity experts to a utility in need to help defend the network or send IT personnel to assist with recovering systems. This program is similar to the way utilities share resources to help restore services after a large storm, but for cyber events.

BOTTOM LINE:

Loss of power to a region has negative economic impacts and may lead to safety issues for the population. Electricity is needed for society's basic needs - water, food, heating/air, medical care, and transportation.

Within the State of Indiana cyber-defense capabilities vary greatly depending on the size of the utility. Smaller utilities are less likely to have dedicated cybersecurity staff and budgets than large utilities. Cyber regulations such as NERC CIP help protect the power grid from commercial malware and normal cyber threat actors.

Additional cybersecurity capabilities are needed to identify, protect, detect, and respond against advance threat actors. As stated in this document, Nation State actors, have targeted the United States power grid. This trend is unlikely to change in the near future. Both government and private industry need to continue working together to make the power grid both resilient and defensible.

---

[7] https://www.wired.com/story/hack-brief-us-nuclear-power-breach/

[8] https://www.thesun.co.uk/news/4915334/russian-hack-attack-on-britain-energy-grid-cyber-crime/

IECC Cyber Vulnerabilities Whitepaper

Water and Wastewater Sector

February 2018

GOVERNOR ERIC J. HOLCOMB'S
INDIANA EXECUTIVE COUNCIL ON CYBERSECURITY

Cyber Vulnerabilities Whitepaper - Water and Wastewater Sector

David B. Tygart
12 February 2018

BACKGROUND:

Many water and wastewater utilities within the State of Indiana, particularly small systems, lack the resources for information technology (IT) and security specialists to assist them with starting and maintaining a cybersecurity program. "Utility personnel may believe that cyber-attacks do not present a risk to their systems or feel that they lack the technical capability to improve their cybersecurity."[1]

The basic problem for water utilities today is the convergence of two systems that used to be relatively segregated: information technology (IT) and operational technology (OT). IT is what a layperson commonly associates with cyber threats: the computer systems that are linked to the internet for email, billing, bookkeeping, and desk work. Viruses enter these systems through a mess of pathways: infected USB drives, email attachments, bad links on compromised websites or even the late night operator linking his iPhone TV to a control computer.[2]

The National Infrastructure Advisory Council, a group of experts that advises the Department of Homeland Security and the president on critical infrastructure, says that cybersecurity awareness among water utilities is "often limited" and that the number of cybersecurity experts in the sector is "insufficient for current needs.[3]

According to the U.S. EPA, Indiana's water and wastewater infrastructure needs a total of nearly $14 billion over the next 20 years to update an aging infrastructure.[4] These costs will compete against the need to improve Cyber Security within this sector.

GOVERNANCE, REGULATORY AND SUPPORT AGENCIES:

Wastewater companies require an annual re-certification of their license to operate, but water companies do not. They use the one they get when they start to operate. New State of Indiana legislation was introduced during the FY18 session. Bill number: SB 362 subject: "Regulation of Water and Wastewater Systems." The bill establishes new requirements for water treatment plants and wastewater treatment plants applying to the Department of Environmental Management for the issuance or amendment of a permit, including a cost-benefit analysis, a capital asset management plan, and a cybersecurity program. Unfortunately, this bill as written might not hit the mark on getting water companies to comply. In addition, as there is no clear standard as to what a "cyber plan" is, not sure if we would get any statewide useful information.

- U.S. Environmental Protection Agency (EPA) - is the designated as the lead agency for the Water and Wastewater Sector.
- Indiana Utility Regulatory Commission (IURC)- Water/Wastewater Division Regulates pricing models and quality of service but stops short of mandating Cyber Defense standards.
https://www.in.gov/iurc/2338.htm

[1] Implementing A Cybersecurity Program At Your Water Or Wastewater Utility; Office of Water (MC 4608-T) EPA, August 2016; https://www.asdwa.org/wp-content/uploads/2016/07/Cybersecurity-Guide-for-States_Final.pdf
[2] http://www.circleofblue.org/2016/world/water-sector-prepares-cyberattacks/
[3] https://www.dhs.gov/sites/default/files/publications/niac-water-resilience-study-slidedeck-qbm-03-14-16-508.pdf
[4] Indiana Utility Regulatory Commission 2016 Annual Report http://www.in.gov/iurc/files/Annual%20Report%202016%20WEB%20version.pdf

- Water and Wastewater Sector Coordinating Council (SCC) - An EPA organized council bringing Federal, State, and local entities, and owners and operators of water utilities together and are responsible for planning and implementing the Sector's security and resilience activities. https://www.waterisac.org/
- Water Information Sharing and Analysis Center, is the designated communications and operations arm of the United States water and wastewater sector. With an all - hazards focus

RISKS:

In the drinking water and wastewater sub-sectors, a cyber-attack could cause chemical contamination, biological contamination and/or physical disruption through the manipulation of specialized computer systems controlling essential infrastructure known as Supervisory Control and Data Acquisition (SCADA) systems. A successful attack could cause major damage, resulting in long periods of operational downtime, financial losses, loss of public trust and most importantly, a threat to public safety.

Unlike the loss of power to the public sector, due to a cyber-attack, the contamination to a public water source thought the manipulation of industrial control systems may go undetected for hours to days having adverse effects on the general population.

PAST ATTACKS:

According to a news report from International Business Times, hackers were able to change the levels of chemicals used to treat tap water during an attack on the outdated IT network of one U.S. plant by exploiting its web-accessible payments system and using it to access the company's control systems.[5]

For eleven days in 2013 an Iranian computer hacker gained access into the computer system that controls Bowman Dam, in Rye, New York. City officials were unaware that they were being hacked until contacted by the Department of Homeland Security. The Iranian computer hacker tapping into the supervisory control and data acquisition system was able to learn water levels and temperatures as well as the status of the sluice gate, which controls the flow of water. Fortunately, the attacker was unable to operate the gate from Iran because that particular control system had been disconnected for maintenance.[6]

SECTOR SPECIFICS:

Most of the water systems in the state are owned by municipal or not-for-profit entities. These entities are managed by a board of directors or town or city councils. According to the 2013 "Water Utility Resource Report: A Look at Indiana's Water Supply & Resource Needs" report prepared by the Indiana Utility Regulatory Commission 487 of 555 utilities surveyed submitted data for evaluation. From the data, 69% are municipal utilities. Not-for-profit and investor owned utilities made up 17% and 11% of respondents, respectively. Conservancy districts, cooperatives, and regional water districts are less common and combined made up less than 4% of respondents.[7] Many industrial businesses self-produce their water and wastewater requirements.

Automation controllers or PLC's within this sector have a long life cycle before replacement 10-20 years. As many of these were designed and install prior to all the cyber concerns many are lacking fundamental blab la

[5] https://www.infosecurity-magazine.com/news/water-treatment-plant-hit-by/
[6] http://www.circleofblue.org/2016/world/water-sector-prepares-cyberattacks/
[7] https://www.in.gov/iurc/files/Water_Utility_Resource_Report-_FINAL-_8282013_with_cover(1).pdf

BOTTOM LINE:

In light of the challenges stated above; aging infrastructure, competition between repairing infrastructure vs improving cyber security and the clear lack of governance as it relates to cyber security leave this sector extremely vulnerable to attack as compared to other critical infrastructure sectors. The results, unlike most other sectors, could have immediate and catastrophic impact on a population. Our approach must be thru outreach and education if we are to see improvements.

IECC Pre- through Post-Incident White Paper

Education Sector

2018

GOVERNOR ERIC J. HOLCOMB'S
INDIANA EXECUTIVE COUNCIL ON CYBERSECURITY

Pre- through Post-Incident White Paper — Education Sector

David Greer, Project Lead the Way
Andrew Korty, Indiana University
William Mackey, Indiana State University
Darryl Togashi, Ivy Tech Community College

BACKGROUND:

The education sector in the State of Indiana consists of a wide range of institutions: K-12 schools, two- and four-year colleges, vocational colleges, and large research universities. While each of these institutions faces similar cyber risks, the resources they have available for a complete cybersecurity program to prepare for, respond to, and recover from cyberattacks are quite variable. Specific gaps, as in most industries, include employee training, robust data backups, and a strong cybersecurity operations function.

Unlike other industries, the education sector has traditionally given broad leeway to faculty, staff, and students to choose their own technology and use it in almost any way they feel appropriate. This culture, present more in higher education than in K-12s, is meant to contribute to academic freedom and the ability to teach, learn, and do research unfettered by excessive policies and technical limitations. While this culture may seem at odds with cybersecurity best practices, the two can coexist peacefully if the business needs and the threat profile of the institution are carefully weighed and considered.

Although the risks in the education sector don't usually result in immediate threats to public safety as they can with some utilities, there are some physical security considerations, especially given the large physical plant of some institutions. The vast computing and communications capabilities of large universities can also be of interest to attackers. But an educational institution's most commonly targeted resource is its stores of personal and institutional data.

GOVERNANCE, REGULATORY AND SUPPORT AGENCIES:

LEVEL	AGENCY/BODY	DESCRIPTION
Federal	U.S. Department of Education	The U.S. Department of Education (US DOE) is responsible for implementing federal laws related to the education system, including students. The agency's primary responsibility is the Elementary and Secondary Education Act (ESEA) of 1965 as amended by the Every Student Succeeds Act (ESSA) of 2015. US DOE is also responsible for various other laws, including[1]: - Family Educational Rights and Privacy Act - Individuals with Disabilities Act - Civil Rights laws, including the Title II of the Americans with Disabilities Act, Title IX of the Education Amendments of 1972, and Title VI of the Civil Rights Act - Workforce Innovation and Opportunities Act

[1] https://www2.ed.gov/policy/landing.jhtml?src=pn

		- Carl D. Perkins Career and Technical Education Act of 2006[2]
Federal	Federal Trade Commission	The Federal Trade Commission (FTC) manages the Children's Online Privacy Protection Act (COPPA) which is a law created to protect the privacy of children under 13. The Act specifies: - That sites must require parental consent for the collection or use of any personal information of young Web site users. - What must be included in a privacy policy, including the requirement that the policy itself be posted anywhere data is collected. - When and how to seek verifiable consent from a parent or guardian. - What responsibilities the operator of a Web site legally holds with regards to children's privacy and safety online, including restrictions on the types and methods of marketing targeting those under 13.
Federal	Federal Communications Commission	As it relates to education, the FCC's ole is related to the governance of the E-Rate program. E-Rate is administered through the Universal Service Administrative Company[3].
Federal	Department of Health and Human Services – Office of Civil Rights	The Department of Health and Human Services' (HHS) Office for Civil Rights is responsible for enforcing the Privacy and Security Rules.
Federal	U.S. Department of Housing and Urban Development	HUD administers the ConnectHome initiative, which is focused on "increasing access to high-speed internet for low-income households". ConnectHome partners with local libraries, schools, private providers, and HUD housing units to fulfil its mission[4].
Federal	U.S. Department of Education, Office of Education Technology	Issues related to technology, infrastructure, and cybersecurity can be found across the many laws and initiatives implemented by US DOE and other federal agencies. However, US DOE has attempted to centralize these issues in its Office of Educational Technology[5]. Guidance and resources on how these laws affect technology issues for both State Education Agencies and Local Education Agencies can be accessed through this office.
State	Indiana General Assembly	Article eight of the Indiana Constitution as amended 2016 states: Knowledge and learning, generally diffused throughout a community, being essential to the preservation of a free government; it shall be the duty of the General Assembly to encourage, by all suitable means, moral, intellectual, scientific, and agricultural improvement; and to provide, by law, for a

[2] https://www2.ed.gov/policy/sectech/leg/perkins/index.html

[3] http://www.usac.org/sl/

[4] https://connecthome.hud.gov/

[5] https://tech.ed.gov/

		general and uniform system of Common Schools, wherein tuition shall be without charge, and equally open to all[6]. The General Assembly therefore establishes laws that: - Grant administrative powers to the State Board of Education; - Prescribe the method of selection, tenure, duties, and compensation of the State Superintendent of Public Instruction; - Manage the Common School fund; - Grant specific authorities to Local Education Agencies, known as School Corporations; and - Establish broad education policies.
State	Indiana State Board of Education	The Indiana State Board of Education (SBOE) is established in Indiana Code Title 20, Article 19, Chapter 2[7]. The SBOE is granted with a host of powers and responsibilities, including the ability and responsibility to adopt administrative rules under IC 4-22-2[8] concerning education policies and procedures as outlined in IC 20-19-2-8[9]. Generally speaking, the duties of SBOE are to: - Establish the educational goals of the state, developing standards and objectives for local school corporations; - Assess the attainment of the established goals; - Assure compliance with established standards and objectives; - Coordinate with the commission for higher education and the department of workforce development to develop entrepreneurship education programs for elementary and secondary education, higher education, and individuals in the work force. - Make recommendations to the governor and general assembly concerning the educational needs of the state, including financial needs; - Provide for reviews to ensure the validity and reliability of the statewide assessment program; and - Oversee the distribution of certain federal aid programs.
State	Indiana Department of Education	Indiana Code 20-19-3 establishes the Department of Education. The State Superintendent of Public Instruction, as established and governed by Indiana Code 20-19-1-1 (IC 20-19-1-1.1 beginning January 10, 2025), is the director of the department. The specific duties and responsibilities of the department are established in both Indiana Code set by the General Assembly and administrative rules adopted by the State Board of Education. Generally speaking, it is the department's responsibility to implement the education laws, policies, and procedures set by

[6] https://iga.in.gov/legislative/laws/const/

[7] http://iga.in.gov/legislative/laws/2017/ic/titles/020#20-19

[8] http://iga.in.gov/legislative/laws/2017/ic/titles/020#4-22-2

[9] http://iga.in.gov/legislative/laws/2017/ic/titles/020/#20-19

		state law and administrative rules. Many of these responsibilities relate to monitoring and supporting local school corporations.
Local	School Corporations	Indiana Code 20-26 defines local school corporations and their powers and duties. The extent to which Indiana favors local control of schools is well represented by IC 20-26-3 – Home Rule, which states: - "Notwithstanding any other law and subject…the policy of the state is to grant to each school corporation all the powers needed for the effective operation of the school corporation."[10] - "The rule of law that any doubt as to the existence of a power of a school corporation must be resolved in favor of the existence of the power."[11] By law, school corporations: 1. **Must** adopt discipline rules that prohibit bullying, which includes bullying that may occur through the use of data or computer software (IC 20-33-8-13.5) and provide training to its employees and volunteers concerning the school's bullying prevention and reporting policy (IC 20-26-5-34.2). 2. **May** offer classes, instruction, or programs regarding the potential risks and consequences of creating and sharing sexually suggestive or explicit materials through cellular telephones, social networking web sites, computer networks, and other digital media.

RISKS:

Educational institutions have large repositories of personal and institutional data, much of which is regulated (see above). Institutions must safeguard this data and the systems that process it while staying true to mission of teaching, research, and community partnership. Many of the safeguards, which include employee training to prevent successful phishing attacks, regularly tested data backup systems to allow recovery from ransomware attacks, highly trained security operations and incident response teams, and others, can be beyond an institution's budget capacity, especially for smaller institutions.

Schools, especially universities, are more akin to cities than companies, with up to 100,000 people using technology independently. As mobile devices and cloud services proliferate, education sector users are becoming ever more independent, and the institution is losing the ability to implement safeguards that can reach all devices and services. Keeping devices secure therefore falls increasingly to the end user, yet due to the sheer number of people involved, training costs escalate quickly. Further, relatively little standardization of training or safeguards exists across the sector, making it difficult to achieve efficiencies through collaboration.

[10] IC 20-26-3-1
[11] IC 20-26-3-2

Few institutions have the budget for a cybersecurity operations center (CSOC), yet given the way technology has changed and threats have evolved, a CSOC is quickly becoming an essential pillar of any cybersecurity program. Gartner writes

> The traditional thinking is that, although the organization does not control the threats, it can control vulnerabilities, and thus, there is a need to focus there. At many organizations, increasing IT complexity and the emergence of bring your own device (BYOD) break down any semblance of control over assets and their vulnerabilities, making vulnerability-centric security much harder, if not impossible. Threat intelligence is a critical tool for enabling the threat-centric side of a security equation and, at least in part, taking the fight to the adversary by identifying, exposing and sometimes prosecuting the threat actors.[12]

The takeaway is that any mature cybersecurity program needs to include cybersecurity operations with a strong threat intelligence component.

But cyberspace isn't the only arena in which cybersecurity funding has an impact. Many colleges and universities have the added responsibility of protecting students that live on campus. While public safety is not a direct concern of cyber risk, many cyber resources are used for life and safety protection. An attacker could target door access control or video surveillance systems to gain access to student living areas and cause harm. Also of concern are blended attacks, in which attackers disable alarm or emergency communication systems just before launching a kinetic attack, thereby increasing damage by reducing the ability of public safety personnel to react and respond.

SECTOR SPECIFICS:

Public and private institutions alike aim to foster an environment of academic freedom, and a traditional, by-the-book approach to cybersecurity is often met with resistance. Particularly in colleges and universities but also in some K-12 environments, CISOs and security practitioners must take a risk-based approach with strict attention to every safeguard's impact on academic and business function. Also, the education CISO's ability to implement safeguards is often constrained by very limited budgets for cybersecurity. These two factors create a unique and challenging cybersecurity environment.

Colleges and universities have shown particular leadership in all types of information sharing, including cybersecurity information. The Research and Education Network Information Sharing Analysis Center (REN-ISAC) consists of 540 member institutions around the world, eight of which are Indiana-based, and is one of higher education's most vibrant information sharing communities. Security practitioners at member schools share threat intelligence, awareness materials, and best practices on a daily basis, and this network of individuals can prove invaluable when coordinating incident response among multiple institutions.

Because of this established culture of information sharing, it's likely that any institution experiencing an incident or attack will request and receive assistance from trusted peers before turning to other groups. It would be rare for educational institutions to accept help from volunteer or National Guard forces in these situations.

PAST ATTACKS:

The 2014 Symantec Internet Security Threat Report puts the educational sector 3rd in number of cyberthreat incidents per year (behind only healthcare and retail)[13]. Since Indiana Code article 24-4.9 requires businesses and other organizations to notify affected consumers following the discovery of a

---

[12] Gartner, *How to Collect, Refine, Utilize and Create Threat Intelligence*, 2016

[13] Symantec Internet Security Threat Report, 2014

personal data exposure as well as the Attorney General's office, we can assume that publicly available data on exposures affecting Indiana educational institutions is reliable.

Indiana educational institutions have reported 29 reported data breach incidents since 2005. That translates into around 3 reported breaches of personal information from Indiana educational institutions each year, for the past 17 years[14]. The data show that, by year, there is not a statistically significant change in the number of breaches. Moving beyond just Indiana, however, 872 breaches have occurred in the education sector alone across the United States, giving us an average of 2.4 breaches per day[15].

Institutions seem to be particularly vulnerable to social engineering campaigns, as a major goal of every university is to foster a sense of 'welcome'. This often times includes allowing students, parents, and friends to bring and connect to their own personal devices. Moreover, student records can become a wealth of lucrative information for potential offenders.

BOTTOM LINE:

As in other sectors, many educational institutions lack the resources to develop and maintain a complete cybersecurity program. Schools that are deficient are particularly vulnerable to threats such as social engineering, ransomware, system intrusions, and denial of service attacks. One of the most commonly reported gaps is in training, in the areas of system maintenance and security (for IT staff), social engineering avoidance, and best practices for data protection. Also typically lacking is a solid security operations program using threat intelligence. As institutions put more resources into cybersecurity, these two areas are likely to receive the most focus.

---

[14] Mackey, *Summary of Questionnaire for Education Sector for the Current State of Cybersecurity in Indiana*, 2018

[15] Center for Digital Education

Indiana National Guard (INNG)
State Cyber Baseline Survey Results

2018

Purpose

This survey was designed to better understand what other states are doing to support these local governments in the support for critical infrastructure cyber protection. The survey was sent through J3 channels to all states and 8 states responded.

Survey Questions:

Many states use their National Guard cyber forces to assist in protecting the networks in their state. According to a National Governors Association (NGA) memo, there were 32 cyber response plans among the 26 states surveyed. In particular California, Michigan, Ohio, and Washington have been working in this area for a number of years. In almost all instances the duty is performed in a state active duty (SAD) status and the soldiers are paid from state funds. Although, Ohio does do some work in non-SAD capacity it is in Inactive Duty Training (IDT) status and the event is geared toward training for their team. The work performed ranges from penetration testing and network vulnerability assessments to assisting local governments, as in Michigan, during the Flint water crisis.

To help develop this document INNG J36 has teamed up with the office of Homeland Security & Public Safety Division NGA Center for Best Practices National Governors Association.

?Q-1. We are interested in finding out if you are conducting vulnerability assessment and/or penetration (PEN) testing with non-DODIN entities within your state? Specifically:

- With whom i.e. State agencies, private companies (critical infrastructure owners) and local governments?
- How are you funding the assessments/PEN testing (SAD, IRT) and who is doing it (DCO-E, CPT, other)?
- How often have you executed those assessments over the past year and the plan sustainable?
- What type of testing, PEN or vulnerability Assessments?
- Do you have TTPs/processes or other information you can share for these engagements.

In Indiana we don't see PEN testing or vulnerability assessments as a "fix all" for the state. We see it more as a way to bring credibility to the need for better awareness and training. We also see it as a way to support the justification to exercise cyber defense within the State's critical infrastructure sectors beyond the energy sector. Our focus currently is with water delivery and election sectors. We are developing plans to exercise these sectors in the next 18-24 months. We will continue participating in the annual GRIDEX Energy sector exercise.

?Q-2. Does your state have a Cyber Response Plan that identifies use of your National Guard assets to assist? Specifically:

- Are you/have you worked with your State on a Cyber Response Plan?

- Is your organization part of the decision making process during a Significant Cyber Incident?
- Have you or are you planning to exercises C2 with the state emergency management teams?

The State Government of Indiana is working to revise its Cyber Response Plan and currently completing the research phase. For the Indiana National Guard we own the "Pre and Post" cyber incident portion of the plan. In the "Pre" phase we are faced with an estimated 8000 entities that could use Cyber assessments. Even if we were to team up with DHS and other private capabilities it is a bridge to far. Not to mention the limitations placed on the DoD under the Economy Act. We see the best use of our limited assets to support outreach as stated above and focus any PEN testing towards State Government agencies. In a "Post" cyber incident scenario we would be in a supporting role to the DHS or other State agencies. Our plan is to develop whole of state government exercises in the future to develop these relationships and processes.

?Q-3. Is your state building capability to response to a significant cyber incident outside of organic capabilities? For example, Michigan has created a volunteer force called the Michigan Cyber Civilian Corps. Maryland is looking to develop their state militia, the Maryland Defense Force.

- Do you have or are you planning to build capability like this in your state?
- If you have what is their strength?
- Have they been used?

Indiana is looking to build additional capability within the Indiana State Police (ISP) by training ISP officers across the state in cyber. We are currently developing concepts and training programs to do this. The advantages we see in placing this in the ISP are legal. Unlike other constructs, the IPS is not limited by as many legal issues as National Guard assets or some other form of a volunteer force.

?Q-4: Are there capabilities identified within your state that you are considering filling with National Guard personnel?

- Are there other areas that you are investigating to support the state's cyber readiness?
- Have you developed working partnerships with Federal/State agencies and what engagements are you using to foster these relationships.

One gap identified in our research is the lack of a cyber analyst in the State's Fusion Center. We are conducting a business case analysis and plan on seeking State funding to fill this capability gap.

California:

Cybersecurity Task Force
The California Cybersecurity Task Force is responsible for identifying, acquiring and establishing funding mechanisms to enhance cybersecurity efforts; promoting actions to enhance cybersecurity; growing the cybersecurity workforce; developing public education; facilitating economic development by promoting a cyber-safe location for businesses and consumers; enhancing cyber emergency preparedness and response; identifying, understanding and sharing cyber threat information; mitigating the cyber risk; and building a comprehensive digital forensics and cyber investigative capability. The task force serves as an advisory body to senior administration officials in matters related to cybersecurity.

NG POC - LTC Jim Parsons, James.L.Parsons@cnd.ca.gov

Q-1 "Assessments/PEN Testing" - CA uses a full time CND-T team funded the State using SAD funding. State law, CA Assembly Bill No 670, which has a standing Network Defense team made up of National Guardsmen paid by state funds that is authorized by the bill to conduct network assessments among other cyber related duties of state agencies and then reimbursed by the agency assessed. CA law requires state agencies to have tests completed every two years and to use state CND-T. Team schedule is full year round.

Q-2 "State Cyber Response Plan" - The state is looking for leadership to oversee a Volunteer Civilian Cyber Force. Incorporates the use of CANG into state response.

Q-3 "State Capacity Building" -

Q-4 "State NG Partnering" -

Georgia:

POC - COL David S. Allen, GAARNG (US) <david.s.allen1.mil@mail.mil>

LTC Anthony (Tony) B. Poole, DCoS, GAARNG (US) <anthony.b.poole.mil@mail.mil>

Q-1 "Assessments/PEN Testing" - In Georgia, we are taking steps to assist the Georgia Technology Authority and Department of Accounts/Audits with vulnerability assessments. These activities will be a mix of SAD/IRT depending on the scope of the work per Deputy Secretary of Defense Policy memorandum 16-002. We are also in preliminary discussions with the Department of Driver Services for PEN testing of their POS system. Our focus currently is with general state agency cyber defense and the energy sector. We are developing plans to exercise the DSCA cyber response process within the next 12-18 months. Our TTPs outside of general cyber incident response are still in development.

Q-2 "State Cyber Response Plan" - The GAARNG has developed a CONPLAN for Cyber Incident Response within the state. This plan was originally developed and published in FY16. This plan provides guidance should the state request support due to a significant cyber incident. The GAARNG is not currently involved in the initial decision making process during such an event. We are developing plans to exercise the DSCA cyber response process within the next 12-18 months. Portions of this plan were exercised during our FY17 Vigilant Guard exercise in conjunction with Title 10 members of the Fort Gordon Cyber Protection Brigade.

Q-3 "State Capacity Building" - The GAARNG is not building a similar capability at this time. We are pursuing initial conversations with certain Cyber Academic Centers of Excellence that may lead to development of a similar capability.

Q-4 "State NG Partnering" - The GAARNG has developed relationships with Federal/State/Local and commercial entities. We currently meet monthly for a cybersecurity working group that includes DHS, FEMA, Secret Service, ICE, Georgia Technology Authority (GTA), and Georgia Bureau of Investigation (GBI). Commercial partners include Metro Atlanta Rapid Transit Authority (MARTA) and Southern Company/Georgia Power. This meeting provides intelligence sharing across the organizations and assists with exercise participation and planning for real-world events. Current efforts include planning for a DSCA Cyber tabletop and the 2019 Super Bowl.

Indiana:

Executive Order: Executive Council on Cybersecurity
This executive order establishes a public-private partnership charged with enhancing Indiana's ability to prevent, respond to and recover from all types of cybersecurity issues, including attacks. The council consists of the homeland security department, CIO, attorney general, adjutant general, state police superintendent, utility regulatory commission chair and others.

NG POC - Mr. David Tygart, Chief Defensive Cyber Programs, david.b.tygart.civ@mail.mil, (317) 247-3323

Assessments/PEN Testing - No test conducted to date. The Indiana National Guards is developing capability and processes to conducted penetration assessments that supports both Internal training objectives and support to State and local government agencies of Indiana thru the Governor's Indiana Executive Council on Cybersecurity. Initially these test will not be to the depth that DHS National Cybersecurity Assessments and Technical Services team (NCATS) conducts but anticipate refining processes and expanding offerings over time. Currently the majority of our assets are deployed and equipment to conduct such testing is in procurement. We plan to have a limited capability in the next 90 days and a robust capability in 180 days.

Q-1 "Assessments/PEN Testing" - We will look at SAD funding and also explore the use of a DoD program called Individual Readiness Training (IRT) that allows use of DOD assets in title 32 status.

Q-2 "State Cyber Response Plan" - Although State legislation was introduced to develop a Volunteer Cyber force construct in Indiana it did not get past committee. Indiana is taking an alternative approach and working to develop a Cyber Taskforce Enforcement Training program to train members of the Indiana State police across the state. The unique advantage to this approach is that it eliminates legal issues other states are facing with a volunteer cyber force. The Indiana will work closely with and augment these teams in the future.

Q-3 "State Capacity Building" - .

State Cyber Plan - Currently in draft form. This plan will creates the Indiana Cyber Advisory Group (CAG). The CAG is a flexible body of emergency management professionals and subject-matter experts that can be scaled to individual cyber incidents. The National Guard is a foundational member.
Q-4 "State NG Partnering" -

Louisiana:

POC - LTC Stephen Durel, Deputy J6, 504-278-8051, stephen.l.durel.mil@mail.mil

Q-1 "Assessments/PEN Testing" - Currently in Louisiana we are not conducting vulnerability however; we are exploring the options with our current state government.

Q-2 "State Cyber Response Plan" - In Louisiana the Governor and TAG have dedicated state and Guard resources to the Cyber defense effort. In December 2017 the Louisiana Governor had formed a 15 member Cyber commission to address the growing Cyber threat to our state at all levels. Additionally the governor in February 2017 tasked his staff, GOHSEP (Governor's Office of Homeland security and preparedness) and the Guard to develop an ESF (Emergency Support Function) -17 that is be specific cyber. Included with this ESF is a Cyber response plan that the Guard help to draft. Currently the Guard with other state and federal agencies is planning a Cyber TTX that will take place in 2019.

Q-3 "State Capacity Building" - Louisiana formed an ad-hoc Cyber team called CDIRT (Cyber Defense Incident Response Team) Louisiana's TAG guidance was to form a Cyber team made up of volunteers from Air and Army DRU's that had IT and Cyber back grounds. The team was formed back in 2013 and conducts quarterly training events at joint Cyber range which LSU manages in a Cyber lab that both GUARD and LSU partnered and built. Once Louisiana was awarded the CPT we filled the positions with CDIRT members which deployed the past March. We are currently leaning forward by rebuilding our cyber team a surge capacity refilling our CDIRT ranks with the next wave of Cyber defenders. Future opportunities.

Q-4 "State NG Partnering" -

We currently we are trying to put intelligence folks into the state fusion center (LA-SAFE) Louisiana state and analytical fusion exchange.
The cyber commission that Louisiana's governor had formed is currently forming sub-committees to identify various cyber issues to include defining each state and federal organizations cyber capabilities' and conducting GAP analysis to fill those needs.
Louisiana has developed several working relationships with both State and Federal partners. The Guard works with GOHSEP in cyber planning, training and conceptual theories. The Guard works with DoA in Cyber planning and execution to include being Co-Leads of the governors proposed Cyber emergency support function (ESF-17). We also work with our state Fusion center (LA-SAFE) with Cyber awareness and information sharing. Members of the CPT and CDIRT work with our federal partners (DHS and FBI) and are members of the FBI Cyber Task Force.

Maryland:

Legislation: Maryland Cybersecurity Council
The council, created in 2015, is responsible for reviewing and conducting risk assessments to determine which local infrastructure sectors are at the greatest risk of cyber-attacks and need the most enhanced cybersecurity measures; assisting private sector cybersecurity businesses in adopting, adapting and implementing NIST framework; recommending a comprehensive state strategic plan to ensure a coordinated and adaptable response to and recovery from cybersecurity attacks; and other responsibilities.
The council is made up of the attorney general (chair), secretary of information technology, secretary of the state police, secretary of business and economic development, adjutant general, executive director of the office of homeland security, the executive director of the development corporation and others.

NG POC - MATTHEW D. DINMORE, Col, MDANG, Joint Staff/J6 Maryland National Guard
matthew.d.dinmore.mil@mail.mil <mailto:matthew.d.dinmore.mil@mail.mil> (443) 927-4011

Q-1 "Assessments/PEN Testing" - One test conducted, future tests planned on a quarterly basis and dependent on ability to sustain these missions. Focus on State agencies. No testing with State critical Infrastructure entities planned currently but it's a high-interest item. Relooking a "joint training" program with both components, state entities, law enforcement, etc. based on several demand signals from state leadership, our state department of IT, and others. TTPs and CONOPS in very rough draft form and will be refined over time. Participation in GRIDEx and other ICS/SCADA activities over the past few years, basic skills and processes developed, future efforts will tie to more engagements. Over the last year+ we've worked with our Maryland Emergency Management Agency (MEMA), Department of IT, and other agencies to build the cyber incident response plan. Version 1 was signed out last year and we exercised it in CYBER PRELUDE.

Q-2 "State Cyber Response Plan" - We have a volunteer cyber unit as part of our state militia, the Maryland Defense Force. The MDDF is part of the military department, so reports to TAG, but falls outside T32 "limits." We integrate the cyber unit into our overall response plan through the joint staff. MD is researching volunteer cyber capabilities, inspired by Estonia's cyber defense league http://www.kaitseliit.ee/en/cyber-unit

Q-3 "State Capacity Building" -
Q-4 "State NG Partnering" -

Michigan:

POC - Matthew LoCricchio, LoCricchioM@michigan.gov (PEN); Dr. Ray Davidson, Office of the CSO Michigan Cyber Civilian Corps, 269.929.2554, DavidsonR5@michigan.gov

Q-1 "Assessments/PEN Testing" - Not being conducting currently but in the planning stages.

Q-2 "State Cyber Response Plan" - MI establish by law a volunteer civilian cyber response force. Costs to oversee the force is estimated at $700k per year and they have 30 personnel signed up to date. They have not been employed as of yet due to unforeseen legal issues. We are also initially limiting ourselves to businesses in the health/medical, educational, and financial sectors, in addition to government entities.

Q-3 "State Capacity Building" - Yes approved plan on the shelf.

Q-4 "State NG Partnering" -

Minnesota:

POC - COL Rick Schute, J3, (651) 268-8931, richard.t.schute.mil@mail.mil

MAJ Chris Brossart, DJ6, christopher.p.brossart.mil@mail.mil

Q-1 "Assessments/PEN Testing" - No, we are not currently doing it, however, it would benefit the state agencies if we provided this type of service. Some work with Critical infrastructure with Excel Energy groups to better understand Industrial Control systems.

Q-2 "State Cyber Response Plan" - Unknown

Q-3 "State Capacity Building" - Not aware that this is happening although we do have the Minnesota Fusion Cell that does include cyber. Not to my knowledge; agency to consider would be Infragard.

Q-4 "State NG Partnering" - This should be answered by MN.IT. I would suggest filling a position in MN.IT, as well as potentially in the MN Fusion Center.

Mississippi:

POC - COL Joe Hargett, G3, Deputy Chief of Staff, (601) 313-6311,

Mccullouch, Murry Brent LTC USARMY NG MSARNG (US) <murry.b.mccullouch.mil@mail.mil>

MAJ Chris Brossart, DJ6, christopher.p.brossart.mil@mail.mil

Q-1 "Assessments/PEN Testing" - The MSNG Defensive Cyber Operations Element (DCOE) has conducted two vulnerability assessments for the Leake County school system and one assessment for the MS Secretary of State's Office. They have not conducted any penetration testing. For the Leake County school, the team conducted an external and internal IP scan. For the Secretary of State's office they conducted an external scan. Team members have been in a drilling status.

Q-2 "State Cyber Response Plan" - Mississippi does not have a Cyber Response Plan. We currently do not have any plans to exercise C2 with the state emergency management teams. The MSNG has had discussions with the MS Information Technology Services department on ways to integrate the Guard's cyber assets with the states' to develop a plan for emergency response.

Q-3 "State Capacity Building" - No.

Q-4 "State NG Partnering" - No.

Missouri:

POC - WO1 Kathleen D. Herrell, Cyber Operations Chief

Q-1 "Assessments/PEN Testing" - no due to legal issues. Passive using cap and rocket SM passive on network. Critical infrastructure not now, but starting to build relationship and trust. Part of Gold tm at CS18 to build trust. Funding is thru T32/CTAA with reservations. Looking for range options .and could use suggestion.

Q-2 "State Cyber Response Plan" - Yes and will exercise this summer.

Q-3 "State Capacity Building" -

Q-4 "State NG Partnering" -

Response Force Construct - looking at Militia discussions started but need legislation first.

Nebraska:

POC - COL Teegerstrom, Eric J, G3, eric.j.teegerstrom.mil@mail.mil

Q-1 "Assessments/PEN Testing" - Nebraska has not conducted any non DODIN assessments. We have been approached by a Public Power District to do a vulnerability assessment and participate in their incident response exercise. We are looking at using our CPT for a Site Assistance Visit as part of their

scheduled training plan on IDT status. Our TAG is working a contract with our University College of Law to review State Law and Federal Statutes about use of cyber. For instance, our State Law provides 'Good Samaritan' protections if a medic provides assistance to the best of their training. Hopefully our Law College will be able to clarify if that same State statue covers a CPT team responding to an event.

Q-2 "State Cyber Response Plan" - Nebraska State government does not specifically identify National Guard assets for cyber response. We do many exercises with our State, but none specifically focused on cyber.

Q-3 "State Capacity Building" - None. Many of our local colleges and universities are working on NSA accreditation and building classes to teach cyber in many areas (IT, Trades, Business) to increase the overall capacity of the Silicon Prairie and our TAG is very supportive of building partnerships with other agencies, however the Nebraska Military Department has not sought to build capacity in this manner.

Q-4 "State NG Partnering" - None at the G6 level.

New York:

POC - CW3 Thomas S. Fancher, NYARNG - Force Integration & Readiness Officer, thomas.s.fancher.mil@mail.mil, (518) 786-4590

Q-1 "Assessments/PEN Testing" - New York currently offers vulnerability assessments to critical infrastructure stakeholders, counties, governmental agencies, and local municipalities. The primary unit responsible for these engagements is the Cyber Support Element (CSE). The CSE is made up of National Guardsman working with the New York Division of Homeland Security and Emergency Services (DHSES). They have conducted 5 vulnerability assessments to date with 4 more scheduled through the summer. In addition, they conduct legislatively mandated site visits to critical infrastructure sites around the state and assist DHSES personnel in assessing the sites cyber security posture. New York Joint Forces Headquarters (JFHQ) G6 office is in the process of standing up a DCO-E to augment the states cyber incident response capabilities with validation at the Cyber Shield exercise next year.

Q-2 "State Cyber Response Plan" - Yes, the NYNG is referenced in the available force pool to the NYS CRP. From our discussions with NYS, NYNG would be used primarily to help maintain and restore (rebuild) functionality while a dedicated NYS CERT entity would conduct DCO. The planning and exercising is in its infancy.

Q-3 "State Capacity Building" - NY is concentrating on achieving functional readiness ratings for its recently activated CPT and reorganized DCOE. There is some capacity in the NY Guard (state militia) but it is not organized presently.

Q-4 "State NG Partnering" - Yes, NYNG has 6 Soldiers on State Active Duty with the NYSDHSES that conduct cyber vulnerability assessments for state and local governments. In addition, NYNG partners with the Army Cyber institute at West Point and the Center for Internet Security in Albany, NY on exercises and training.

North Dakota:

POC - COL James R. Olson, G3, james.r.olson.mil@mail.mil, W: 7013333090

Q-1 "Assessments/PEN Testing" - North Dakota is not conducting vulnerability assessments nor penetration testing with outside agencies. While we see this as a possible area of support for our mission partners, our cyber assets are currently not robust enough to accomplish this task. We continue to

participate in any and all exercises and Cyber working groups that are available to us, but the capabilities in this question will likely be more robust upon return of our Cyber Protection Team from its mobilization in early 2020. However, for this capability to exist in the future, it is paramount that our legal resources receive the training necessary for our forces to operate in this space.

Q-2 "State Cyber Response Plan" - Working - North Dakota is participating in a Cybersecurity Task Force called by the Director of Homeland Security. We are meeting with private business, utilities and State government to examine 15 of the 16 critical infrastructures (ND does not have nuclear). The end result of this Task Force is to develop an Incident Response Plan for North Dakota. We continue to feel our role largely amounts to a Coordinate Train Advise and Assist role as per the Secretary of Defense CTAA memo. We are working with colleges and universities to help shape cyber education, as well as assisting with general cyber education via conferences and workshops. Again in a CTAA role, our CPT has the capability to work with various entities to assist with cyber training and best business practices.

We don't have a Cyber Response Plan at this point, but do have an internal Incident Response Plan. We will be initiating work on a Cyber Annex to our All Hazard Response Plan in the near future.

Q-3 "State Capacity Building" - Interested - While we are not currently working to build this type of capability within North Dakota, it is certainly something in which we are interested. As per our response to Question #2, our work with the ND Task Force may lead to this type of capability once we have examined not only the capabilities within our state, but also the areas where our capabilities are not as robust.

Q-4 "State NG Partnering" - none - At this time, North Dakota is not looking to fill any other positions with National Guard personnel. Our State Fusion Center has a Cybersecurity analyst on staff from the North Dakota Information Technology Department. He is leading the Task Force mentioned in Question #2, and we have a very good relationship with him and his team. We continue to ensure our mission partners see the North Dakota National Guard as a viable resource like they would during any natural disaster. Our work in bringing together private and public educational institutions, private business and State and Federal resources has proven to be a very effective model.

Ohio:

POC - Mamula, Kevin T MAJ Cyber Lead, kevin.t.mamula.mil@mail.mil; Teri Williams , LTC J6/G6 / DoIM 346-7249 (614) 336-7249 teri.d.williams.mil@mail.mil

Q-1 "Assessments/PEN Testing" - The OHNG cyber team has conducted 12 assessments so far and plan to increase that number to 12-16 per year. Funding is provided by the State using SAD. Focus is on State cabinet/administrative departments currently. Other agencies can request support thru the governor's office. Actively conducting PEN testing, 12 so far, plan for 12-16 per year. Each test take 2 weeks and consist of Intel gathering, phishing e-mail and physical security breach attempts, followed by actual PEN testing and final report. No testing with State critical Infrastructure entities currently, plans underway to move towards this. TTPs and CONOPS in draft form.

Q-3 "State Capacity Building" -
Q-4 "State NG Partnering" -

Response Force Construct - OH is developing a Cyber Reserve that will work for the Governor and is nested under the TAG. This differs from the MI Civilian reserve force, unlike MI force that is managed by the state, the OH force will be managed by the TAG.

Q-2 "State Cyber Response Plan" -

Utah:

Legislation: Data Security Management Council
This law created the Data Security Management Council to review existing state government data security policies, assess ongoing risks to state government, create a method to notify state and local government entities of new risks, coordinate data breach simulation exercises and conduct other cybersecurity related activities. The council consists of the chief information officer, an individual appointed by the governor, an individual appointed by the speaker of the House of Representatives and the highest-ranking IT official from the judicial council, the board of regents, the office of education, the Utah College of Applied Technology, the state tax commission and the office of the attorney general.

NG POC - COL Paul S. Peters, G3/5/7
CW4 Rick Gardner, Deputy CIO / G6, Utah Army National Guard, O: 801-432-4111, C: 801-716-9129

Q-1 "Assessments/PEN Testing" - Utah has offered assessments as a "Force Package" that the governor could call on. As of today we have not conducted PEN testing or vulnerability assessments. It is anticipated that assessments would be in a SAD status. Both would be conducted by the DCOE.

Q-2 "State Cyber Response Plan" - Utah Department of Emergency Management (DEM) does have an All Hazards Response Plan with a Cyber Annex. The annex list and describes the UTNG DCOE as a resource for cyber incident response. We worked closely with DEM to develop the Annex and continue to coordinate with them and participate in table top exercise, in fact the next TTX is scheduled for 12 April. It will involve DHS, DEM, and Water/Waste Water Critical Infrastructure partners.

Q-3 "State Capacity Building" - Yes, Utah is in the exploratory phases of developing a Civilian Cyber Corps.

Q-4 "State NG Partnering" - Currently the DCOE collaborates and has working relationships with Utah Department of Technological Services, Utah DEM, State Attorney General's Office, Department of Homeland Services, FBI, local academia, and private sector partners.

Engagements include Key Leader engagements, regularly scheduled committee meetings, Table Top Exercises, Cyber Shield Exercise, training opportunities, JAG/Legal Counsel discussions, and consultation on cyber related activities.
NOTE: Has Cyber Forensics Team imbedded in its Counter Drug Program.

Virginia:

NG POC - LTC Terry Duran, Cyber Planner, (703) 995-7023

Q-1 "Assessments/PEN Testing" -

Response Force Construct -

http://vdf.virginia.gov/2016/12/19/vdf-serves-as-technical-lead-for-ongoing-cyber-assessment-mission/

Q-2 "State Cyber Response Plan" -

Q-3 "State Capacity Building" -

Q-4 "State NG Partnering" -

Washington State:

NG POC - Thomas A. Pries, Lt Col, WA ANG, J-36 Cyber Operations Plans, thomas.pries@us.af.mil
Comm: 253-982-1689

Q-1 "Assessments/PEN Testing" -

3/29/18 - No Pen tests on our side currently. We do offer this service and have done so in the past, but all of our customers are really more interested these days in a survey mission where we produce a relational model and Risk Mitigation Plan. Last mission was 10 guys for 3 weeks. Cost to customer was $70K, executed in SAD. Looking to do a repeat in T-32 next time around under CTAA, likely next winter some time if resources allow. Currently have one other mission in the planning stage that we'll execute in T-32 later this summer.

We have 2 CPT's in-state, and 3 additional Cyber to Physical System teams of 10 people each (currently manned at about 65%). Given this, we could comfortably support two missions per year and still meet our T-10 work load. We're definitely the anomaly though as I don't know of any other state that has that much resource to pull from. Our CPT's are heading into dwell over the next 18 months though so that'll limit availability somewhat.

11/1/17 - We are actively engaged in security assessments with both local government and private entities. However, our assessment method is a bit broader than just pen testing in that it follows the Air Force CPS (Cyber to Physical Systems) methodology. We offer a menu of options to our customers of which a traditional pen test is one item on the menu among others. Depending on what they feel best meets their goals we then scope the mission accordingly.

State National Guard Cyber Baseline

as of 27 April 2018

	POC	assesments past yr	Assesments planned / yr	Funding	Focus on (Gov Agencies)	Focus (Critical Infstr)	Note	CPT, CO BN pax	State Cyber Respons Plan	Response Force (Vol Civ other Cyber)
Alabama								11		
Alaska										
Arizona										
Arkansas								7		
California	LTC Jim Parsons	12	12	SAD	Yes	No	Full time team state funded with SAD	39	Yes	Civ Vol planned
Colorado								11		
Connecticut								9		
District of Columbia										
Delaware										
Florida										
Georgia	COL David Allen, G3 LTC Tony B. Poole, DCoS	0	Planning	SAD/IRT	Yes	Yes	Planning stage - Focus on state agency cyber defense and energy sector	39	Yes	None
Guam										
Hawaii										
Idaho										
Illinois								18		
Indiana	Mr. David Tygart, J36	0	6-12	SAD/IRT	Yes	Yes	IRT will br first Cyber request to NGB	11	Draft	ISP planed
Iowa	CPT Robert Randol									
Kansas										
Kentucky	SSG scott Paige, 175 CPT	0	0	NA	No	No	Focus on T10 mission	14		
Louisiana	LTC Stephen Durel, Deputy J6	0	0	NA	Future	No		18	Draft	AF#ARNG Response Team
Maine								11		
Maryland	COL Matthew Dinmore, J6	1	2	SAD			Vulnerability Assessment focus	39	Draft	Militia 20(+)
Massachusetts								53		
Michigan	Dr. Ray Davidson - Vol Cyber Force	No	No	NA	Yes	No		14	Yes	Civ Vol 30
Minnesota	COL Rick Schute, J3 MAJ Chris Brossart, DJ6	0	0	NA	NA	NA	Pending return of DCO/CPT leads	39	unk	unk
Mississippi	COL Joe Hargett, G3	2	unk	T32 Drill	Yes	Yes		7	No	None
Missouri	WO1 Kathleen D. Herrell, Cyber Op	2	2	SAD	Yes		Vulnerability Assessment focus, Full time tech March 2018	21		Militia (?)
Montana										
Nebraska	COL Teegerstrom, Eric J, G3	0	0	NA	NA	NA	Looking at using our CPT for a Site Assistance Visit	11	No	unk
Nevada										
New Hampshire								13		
New Jersey								14		
New Mexico										
New York	CW3 Thomas S. Fancher	6	10	SAD	Yes	Yes	6 full time SAD working with NYSDHSES	25	Yes	none
North Carolina										
North Dakota	COL James R. Olson, G3	0	0	NA	NA	NA	Not robust enough, after 2020. Legal unresolved	7	No	none
Ohio	MAJ Kevin Mamula, Cyber Lead	8	12-18	SAD/T32 CTAA	Yes	No	Focus on State Govrn Agencies PEN testing	14	Yes	Civ Vol planed
Oklahoma										
Oregon										
Pennsylvania										
Puerto Rico										
Rhode Island										
South Carolina								95		
South Dakota								7		
Tennessee								14		
Texas								14		
Utah	COL Paul S. Peters, G3/5/7 CW4 Rick Gardner D CIO / G6	0	0	SAD assumed	NA	NA	Cyber Forensics Tm in Counter Drug	14	Yes	Exploring Civilian Cyber Corps
Vermont								9		
Virginia	LTC Terry Duran, Cyber Planner	10+		SAD	Yes	Yes	Vulnerability Assessment focus state loc govn, schools. . .	271		VA Defense Force Militia
Virgin Islands										
Washington	Lt Col Thomas Pries, J-36	0	2	SAD/T32 CTAA	Yes	Yes	Focus on Risk Mitigation Plans not PEN	39 AF	Yes	