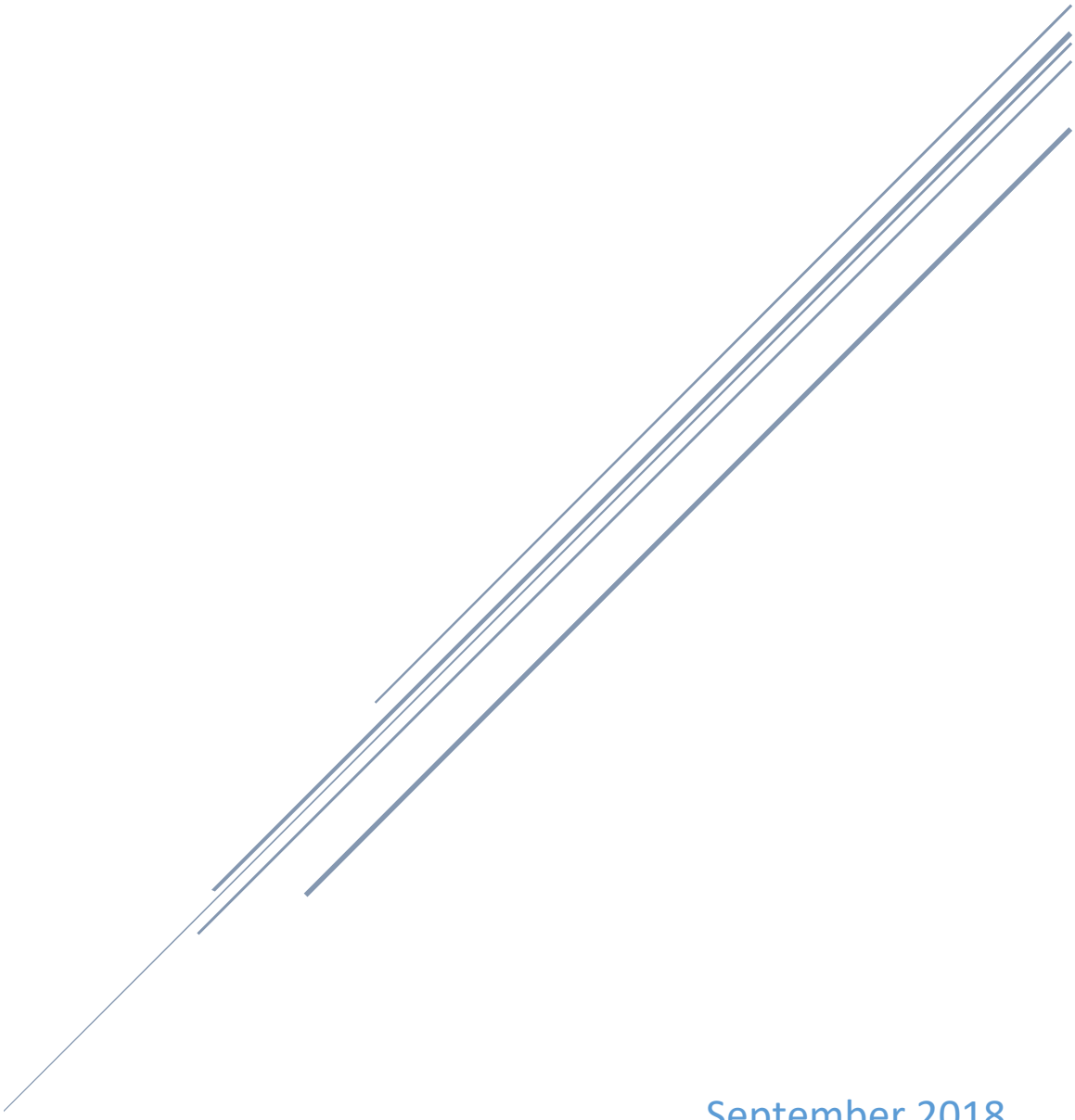
# COMMUNICATIONS COMMITTEE STRATEGIC PLAN

Chair: Joni Hart | Co-Chair: Dan Solero



September 2018

Indiana Executive Council on Cybersecurity

# Communications Committee Plan

# Contents

# Committee Members

## Committee Members

| Name | Organization | Committee Position | IECC Member Type |
|---|---|---|---|
| Joni K. Hart | Broadband Innovation Group | Chair | Voting |
| Daniel J. Solero | AT&T | Co-Chair | Voting Proxy |
| John Greene | New Lisbon Telephone Company | Full time | Advisory |
| James Haley | City of Fort Wayne | Full time | Advisory |
| Benjamin Marrero | Ivy Tech Community College | As needed | Advisory |
| Barry Ritter | Indiana Statewide 911 Board | Full time | Advisory |
| Rami Mohamad Salahieh | Ivy Tech | As needed | Advisory |
| David Vice | Integrated Public Safety Commission | Full time | 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**
  - Definition: Determine how various stakeholders and organizations define the Communications Sector nationally and locally.
  - Relationships: Determine key relationships between public and private sector stakeholders driven by existing frameworks, such as National Security Telecommunications Advisory Committee (NSTAC), National Coordinating Center for Communications (NCCC), Department of Homeland Security (DHS), and private sector initiatives.
  - Responsibilities: Determine what rules and practices govern the cybersecurity activities of sector stakeholders and players in terms of regulation, legislation, and accepted best practices.
  - Cross-Sector Planning: Determine what unique characteristics of the Communications Sector environment present opportunities for better cross-sector planning and understanding.
  - Opportunities: Determine what threats, market opportunities and technology advancements are driving cyber security activities in the communications sector.

- **Research Findings**
  - Definition: The sector is generally accepted to be consistent with the definitions used at the Federal level by organizations such as the Department of Homeland Security (DHS) and the National Security Telecommunications Advisory Committee (NSTAC).
  - Relationships: Sector members in the private sector partner on many public policy issues through organizations such as the Broadband Innovation Group, the Indiana Broadcasters Association (IBA), the Indiana Broadband and Technology Association (IBTA), National Security Telecommunications Advisory Committee (NSTAC), the Communications Information Sharing and Analysis Center (known as NCC), and similar cross-industry associations and government-sponsored bodies.
  - Responsibilities: The Communications Sector features a diverse landscape of regulatory and legislative responsibilities at all levels (local, State, National, and International). At the State level, the Indiana Utility Regulatory Commission (IURC) provides regulatory oversight to a vast swath of the Communications Sector. At the Federal level, the Federal Communications Commission provides similar oversight. Cybersecurity responsibilities are additionally stipulated through a matrix of Federal and State bodies as authorized by State and Federal law. Across all sectors, the US-CERT National Cyber Incident Response Plan lays out many key roles and responsibilities that map into a broader Federal response framework.
  - Cross-Sector Planning: Many stakeholders in the Communications Sector operate both at the national and international levels. These organizations are afforded opportunities to participate directly in industry and government associations like National Security Strategy (NSS), NSTAC, and various related organizations. Sector members who operate more locally within the State may benefit from a more cohesive partnership coordinated through the Multi-State Information Sharing and Analysis Center (MS-ISAC).

- Opportunities: Information sharing continues to drive much of the cybersecurity coordinated planning across the sector and with other industry and public stakeholders. Specific technology-driven innovations that enable a faster response may offer opportunities to deepen these partnerships and drive to a more cohesive and effective partnership architecture.

- **Committee Deliverables**
  - Communications Sector White Paper
  - Cyber Contact Lists
  - Cyber Incident Response Engagement Guidance

- **References**
  - DHS Critical Infrastructure Sector-specific Overview: https://www.dhs.gov/communications-sector
  - DHS 2015 Sector-specific Plan: https://www.dhs.gov/sites/default/files/publications/nipp-ssp-communications-2015-508.pdf
  - National Council of ISACs: https://www.nationalisacs.org/member-isacs
  - Burning Glass Technologies: http://burning-glass.com
  - US-CERT National Cyber Incident Response Plan: https://www.us-cert.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf
  - Multi-State ISAC (MS-ISAC): https://www.cisecurity.org/ms-isac/
  - National Security Telecommunications Advisory Committee (NSTAC): https://www.dhs.gov/national-security-telecommunications-advisory-committee
  - Indiana Office of Utility Consumer Counselor: http://www.in.gov/oucc/2492.htm
  - National Center for Systems Security and Information Assurance (CSSIA): http://www.cssia.org/
  - CyberSeek.org: http://cyberseek.org/heatmap.html
  - Indiana Utility Regulatory Commission: http://www.in.gov/iurc/
  - Federal Communications Commission: http://www.fcc.gov
  - Broadband Innovation Group: http://broadbandig.org/
  - Indiana Broadcasters Association: https://www.indianabroadcasters.org/

# Research

## Research

1. **What has your area done in the last five years to educate, train, and prepare for cybersecurity?**
    a. The communications sector has been at the forefront of cybersecurity research, innovation, response planning, and cross-industry coordination. Industry companies participate in many DHS charter organizations, such as the Communications Sector Coordinating Council, where 35 communications sector companies work in partnership with DHS to define priorities and protection objectives for National Critical Infrastructure. Similarly, the Communications ISAC (NCC) and the National Security Telecommunications Advisory Committee (NSTAC) feature robust public/private partnerships aimed at furthering the National strategic approach to protecting critical infrastructure relates to the communications sector.
    b. Private companies in the communications sector compete for cybersecurity workforce resources with all other sectors. Talent shortages continue to drive innovative approaches to continuing education and skillset pivots in the existing workforce. Many organizations encourage and share cost for college degree programs in computer science and cybersecurity. AT&T, as an example, has taken the additional steps of developing robust internal certification curriculums in order to organically grow a market-competitive workforce.
    c. Additionally, communications sector companies invest in cybersecurity research programs with a wide array of public and private higher education institutions. In 2016, AT&T sponsored a cybersecurity case study competition at Indiana University. Additionally, many K-12 schools participate in the Air Force Association's Cyber Patriot National Youth Cyber Education Program, of which AT&T is a Diamond Sponsor. Coaches across the country come from all sectors, including communications.
    d. A committee member works at Ivy Tech Community College as full-time assistant professor teaching Cyber Security and Information Assurance. He offers a view of how higher education institutions can help lead the way in training and education: Ivy Tech has been designated a National Center of Academic Excellence in Information Assurance 2-Year Education by the National Security Agency and the Department of Homeland Security. https://news.ivytech.edu/2012/05/21/ivy-tech-community-college-designated-center-of-academic-excellence-in-information-assurance/
    e. Ivy Tech has a cybersecurity student club on campus where students meet weekly and train for Cyber Security state, national, and international competitions such as:
        i. National Cyber League (NCL) https://www.nationalcyberleague.org/
        ii. US Cyber Challenge (USCC) http://www.uscyberchallenge.org/
        iii. Colligate Cyber Defense Competition (CCDC) http://www.cssia.org/ccdc/
        iv. National Security Agency (NSA) Codebreaker Challenge https://nationalccdc.org
    f. Ivy Tech also provides cybersecurity awareness for the community during the National Cyber Security Awareness Month sponsored by Department of Homeland Security and invited Cyber Security IT Professionals and Law Enforcement Agencies

Forensic Intelligence analyst to speak to our students, faculty, staff, and the public "about Cyber Security awareness."

g. Other organizations represented by committee members also volunteer to provide Cyber Security Awareness information across public events, typically in coordination with Cyber Security Awareness activities in October.

**2. What (or who) are the most significant cyber vulnerabilities in your area?**

a. For the communications sector in a general sense, vulnerabilities that have the potential to reduce or significantly impair service pose the greatest risk. Many communications services rely on the ability to transmit information in near real time. Any disruption to these services can have a vast impact on the public and to critical safety and private industry activities. As such, the class of threats generally known as Denials of Service or Distributed Denials of Service (DDoS) are extremely significant within the communications sector.

b. Also, vulnerabilities that could lead to information disclosure are significant and extremely important. Loss of customer information (CPNI), intellectual property, business plans, and information that could lead to a threat actor being able to compromise operational practices all fall into this category and are generally related to information technology (IT) infrastructure security.

c. Finally, a class of cybersecurity vulnerabilities that lead to fraudulent consumption of pay services tends to be important to the communications sector.

**3. What is your area's greatest cybersecurity need and/or gap?**

a. Sharing of threat information across public and private sector boundaries and within the broader sector continues to be of critical importance. Significant improvements have been made over the past fifteen years. However, there is still a lot of room for additional improvement.

b. Some hard and soft barriers to making effective use of information sharing in the communications sector are at play: For starters, the use of technology to enable rapid information sharing is available, but not close to universal adoption. The Structured Threat Information eXpression (STYX) and Trusted Automated eXchange of Indicator Information (TAXII) protocols for threat information sharing have helped by enabling technologies to communicate at machine speed. However, coordination and response still occurs largely at human speed, and often with significant organizational latency. Additional investment in and adoption of cyber response automation is needed across the sector.

c. The communications sector is also made up of a complex blend of regulatory and legally mandated responsibilities that do not easily keep up with the pace of cyber threats and exploits. A simplification of this landscape could help accelerate cyber response times.

d. Finally, organizational latency can likely be reduced by simplifying or reducing penalties associated with cybersecurity operational practice. In order for responses to proliferate through the sector at the speed of an attack, organizations must be made to feel empowered to take action without needing to evaluate the risk of penalty for acting or sharing on information that is not otherwise compulsory.

**4. What federal, state, or local cyber regulations is your area beholden to currently?**

a. The regulated portion of the communications sector is regulated at the State level by the Indiana Utilities Regulatory Commission and at the Federal level by the Federal Communications Commission. At the Federal level, the following are major pieces of legislation that govern the sector:

   i. The Communications Act of 1934

   ii. The Cable Communications Policy Act of 1984

iii. The Cable Television Consumer Protection and Competition Act of 1992
iv. The Telecommunications Act of 1996

b. Public policy implementation has been guided by and interpreted broadly by the FCC as well as in United States case law, such as *Comcast Corp. v. FCC (2010).*
c. Title 170 of the Indiana Administrative Code establishes the framework through which the IURC operates to develop and adopt rules and regulations concerning practice, procedure, and standards of service.

5. **What case studies and or programs are out there that this Council can learn from as we proceed with the Planning Phase?**
    a. The United States Department of Homeland Security is home to many programs and bodies that deal with whole sector and whole nation cybersecurity planning, information sharing, and response activities. Indiana and sector members across the spectrum already participate in most of these programs.
    b. Key programs from which this Council can learn include but are not limited to: The DHS Sector-Specific Plans, MS-ISAC, NCC, NSTAC, and NCIRP. These are all mature programs intended to foster public/private partnerships across a range of activities, including cyber defense and planning.

6. **What research is out there to validate your group's preliminary deliverables? This could be surveys, white papers, articles, books, etc. Please collect and document.**
    a. Article outlining the value of early cyber education in Israel: https://www.dailynews.com/2017/02/04/in-israel-teaching-kids-cyber-skills-is-a-national-mission/
    b. DHS 2015 Sector-specific Plan: https://www.dhs.gov/sites/default/files/publications/nipp-ssp-communications-2015-508.pdf
    c. US-CERT National Cyber Incident Response Plan: https://www.us-cert.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf
    d. Johns Hopkins Applied Physics Laboratory paper on a Cybersecurity framework known as Integrated Adaptive Cyber Defense (IACD): https://secwww.jhuapl.edu/IACD/Resources/OnePagers/Autoimmunity-for-CTI-Sharing-One-Pager-200.pdf
    e. BurningGlass.org Cybersecurity job market analysis: http://burning-glass.com/wp-content/uploads/Cybersecurity_Jobs_Report_2015.pdf
    f. War on the Rocks article on the Cyber Security workforce gap as a National Security concern: https://warontherocks.com/2017/05/the-cyber-workforce-gap-a-national-security-liability/
    g. ISC2 Article on the growing Cyber Security workforce gap: http://blog.isc2.org/isc2_blog/2017/02/cybersecurity-workforce-gap.html

7. **What are other people in your sector in other states doing to educate, train, prepare, etc. in cybersecurity?**
    a. Many Colleges and Universities in other states are starting to become a Center of Academic Excellence in cyber education. Here is the current list by the NSA/DHS:
        i. https://www.cybersecuritymastersdegree.org/dhs-and-nsa-cae-cd-designated-schools-by-state/
    b. Also, other states Colleges and Universities have on campus Cyber Security Club and Cyber Security Training Centers. To mention a few for example are DePaul University and Moraine Valley Community College.

i. DePaul University Cyber Club is a leader in Cyber Security Competition: https://www.depaulnewsline.com/debuzz/depaul-cyber-security-team-places-third-national-competition
ii. Moraine Valley Community College is a leader in Cyber Training: https://www.morainevalley.edu/news-story/hub-for-cybersecurity-training-at-moraine-valley/

8. **What does success look like for your area in one year, three years, and five years?**
    a. One year success should be measured in terms of getting sector roles, responsibilities, and partnerships across public/private and intra-sector boundaries clarified and simplified as related to cyber planning and response. Heading into 2019, there should be significant momentum towards more effective partnering in real time operational actions bolstered by clear and tested operational planning.
    b. Three-year measures of success should include a significant reduction in organizational latency in these partnerships, which should be achieved through technical, operational, and public policy improvements.
    c. Across all sectors, we believe that a critical measure of success in five years is a significant closing of the cybersecurity skills gap in the workforce. This may present an economic development opportunity for Indiana, and it is crucial for the long-term viability of all industries.

9. **What is the education, public awareness, and training needed to increase the State's and your area's cybersecurity?**
    a. Recommendations:
        - We do not know of any schools in Indiana that are a CAE Center of Academic Excellence in Cyber Operations. So Indiana has no CAE in CO yet. Please see the list below for the entire USA: https://www.nsa.gov/resources/educators/centers-academic-excellence/cyber-operations/centers.shtml
        - We do not know of any schools in Indiana that are a National Center for Systems Security and Information Assurance (CSSIA). This is critical for training Indiana faculty, Students, and the public in Cyber Education. For Example, Illinois has CSSIA at Moraine Valley Community College. http://www.cssia.org/
        - We believe that we need to provide early public cybersecurity education starting at K-12, please see this article. https://www.edweek.org/ew/articles/2017/03/22/with-hacking-in-headlines-k-12-cybersecurity-ed.html
          Also, we need to promote and involve many k-12 schools in cyber education training. https://www.k12cybersecurityconference.org/
          Furthermore, public schools should be encouraged to consider participating in the Air Force Association's Youth Cyber Education Program, called Cyber Patriot: https://www.uscyberpatriot.org/
        - We recommend that we must make it a mandatory part of our College Education in Indiana for students attending college to take a course in cybersecurity awareness. Please see this article about early cybersecurity education in Israel. https://www.dailynews.com/2017/02/04/in-israel-teaching-kids-cyber-skills-is-a-national-mission/

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?**

burningglass
CAREERS IN FOCUS

## Appendix 1: State Data

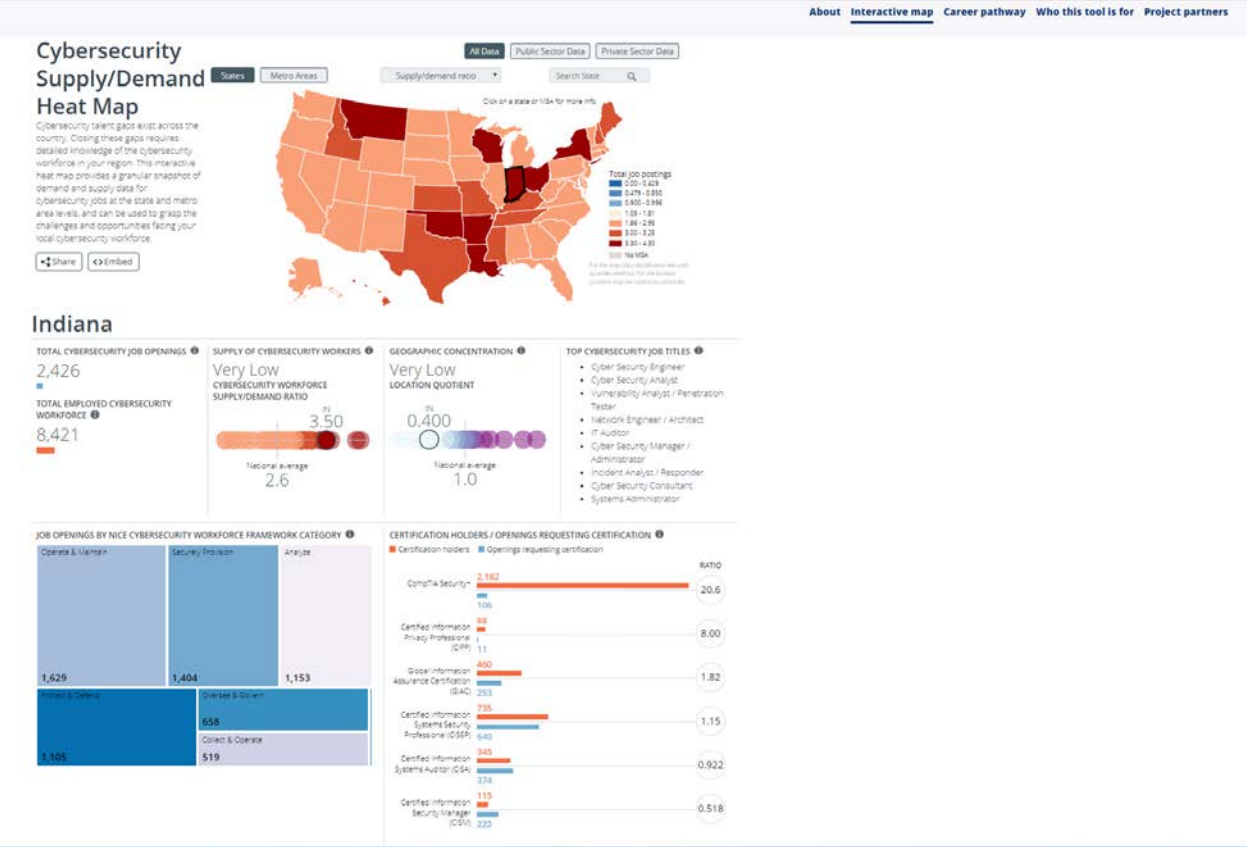
| | State | Total Postings | Location Quotient* | % Growth (2010-2014) |
|---|---|---|---|---|
| 1 | Alabama | 2,159 | 0.66 | 31% |
| 2 | Alaska | 556 | 1.00 | 17% |
| 3 | Arizona | 5,502 | 1.18 | 87% |
| 4 | Arkansas | 989 | 0.5 | 117% |
| 5 | California | 28,744 | 1.02 | 75% |
| 6 | Colorado | 7,688 | 1.77 | 111% |
| 7 | Connecticut | 2,771 | 0.97 | 98% |
| 8 | Delaware | 1,152 | 1.67 | 92% |
| 9 | Florida | 9,847 | 0.67 | 135% |
| 10 | Georgia | 8,757 | 1.22 | 121% |
| 11 | Hawaii | 1,364 | 1.31 | 39% |
| 12 | Idaho | 634 | 0.53 | 260% |
| 13 | Illinois | 11,428 | 1.16 | 163% |
| 14 | Indiana | 2,347 | 0.48 | 139% |
| 15 | Iowa | 1,951 | 0.74 | 158% |
| 16 | Kansas | 1,654 | 0.71 | 168% |
| 17 | Kentucky | 1,753 | 0.58 | 209% |
| 18 | Louisiana | 1,563 | 0.48 | 275% |
| 19 | Maine | 791 | 0.74 | 214% |
| 20 | Maryland | 11,406 | 2.40 | 39% |
| 21 | Massachusetts | 7,911 | 1.45 | 92% |
| 22 | Michigan | 4,225 | 0.59 | 117% |
| 23 | Minnesota | 4,059 | 0.88 | 98% |
| 24 | Mississippi | 827 | 0.45 | 161% |
| 25 | Missouri | 4,004 | 0.86 | 88% |

| | State | Total Postings | Location Quotient* | % Growth (2010-2014) |
|---|---|---|---|---|
| 26 | Montana | 344 | 0.43 | 189% |
| 27 | Nebraska | 1,603 | 1.00 | 68% |
| 28 | Nevada | 1,462 | 0.70 | 89% |
| 29 | New Hampshire | 581 | 0.50 | 134% |
| 30 | New Jersey | 8,268 | 1.21 | 80% |
| 31 | New Mexico | 1,003 | 0.72 | 119% |
| 32 | New York | 14,089 | 0.97 | 104% |
| 33 | North Carolina | 7,503 | 1.06 | 127% |
| 34 | North Dakota | 322 | 0.49 | 341% |
| 35 | Ohio | 6,281 | 0.72 | 141% |
| 36 | Oklahoma | 1,476 | 0.53 | 196% |
| 37 | Oregon | 2,618 | 0.89 | 136% |
| 38 | Pennsylvania | 5,745 | 0.59 | 69% |
| 39 | Rhode Island | 1,267 | 1.53 | 134% |
| 40 | South Carolina | 2,312 | 0.69 | 134% |
| 41 | South Dakota | 354 | 0.50 | 195% |
| 42 | Tennessee | 2,340 | 0.51 | 97% |
| 43 | Texas | 18,525 | 0.92 | 113% |
| 44 | Utah | 1,371 | 0.61 | 146% |
| 45 | Vermont | 281 | 0.52 | 168% |
| 46 | Virginia | 20,276 | 3.09 | 38% |
| 47 | Washington | 5,119 | 0.96 | 94% |
| 48 | West Virginia | 496 | 0.41 | 35% |
| 49 | Wisconsin | 2,429 | 0.51 | 139% |
| 50 | Wyoming | 176 | 0.37 | 245% |

*Location quotients show how concentrated demand is in a particular geography relative to employment in that area. National location quotient equals 1.0; an LQ of 1.2 indicates that demand is 20% more concentrated than nationally.




a. Since wide swaths of the communications sector operate both nationally and internationally, the workforce statistics specific to Indiana cybersecurity-related jobs presents a misleading picture of the sector's preparedness to plan for and respond to events. We've provided a more generalized assessment of the workforce challenges that appear to be universally impactful across sectors:
    i. By researching online and reading the report that is published by Burning glass at Job Market Intelligence Cyber Security Jobs as of 2015, we noted that there is a total posting of 2,347 cybersecurity jobs with Location Quotient of 0.48 and Growth Percentage of 139% between 2010 to 2014. http://burning-glass.com/wp-content/uploads/Cybersecurity_Jobs_Report_2015.pdf
b. Also, according to the article "THE CYBER WORKFORCE GAP: A NATIONAL SECURITY LIABILITY?", which clearly indicates the widespread issue, Indiana's gap is wider than the US average.
    a. "Current data shows a talent shortfall of 40,000 unfilled cybersecurity jobs per year in the United States, with a growing international talent gap to match."
    b. https://warontherocks.com/2017/05/the-cyber-workforce-gap-a-national-security-liability/
c. The entire world also has a shortfall of workers "CYBERSECURITY WORKFORCE SHORTAGE PROJECTED AT 1.8 MILLION BY 2022" according to this website http://blog.isc2.org/isc2_blog/2017/02/cybersecurity-workforce-gap.html
d. Finally, according to CyberSeek.org interactive map, it shows that the supply of cybersecurity workers in Indiana is at Very Low with cybersecurity workforce Supply/Demand Ratio at 3.5 (see image below):




**Indiana Data between October 2016 through September 2017**

e. TOTAL CYBERSECURITY JOB OPENINGS: 2,426
   a. Shows the number of online job listings for cybersecurity-related positions
f. TOTAL EMPLOYED CYBERSECURITY WORKFORCE: 8,421
   a. Shows the estimated number of workers employed in cybersecurity-related jobs in 2016. This includes workers in primary cybersecurity jobs – such as cybersecurity analysts – as well as workers in roles requiring cybersecurity-related skills and certifications to capture the full potential cybersecurity workforce.
g. Please see the above interactive map at: http://cyberseek.org/heatmap.html

**11. What do we need to do to attract cyber companies to Indiana?**

a. If all traditional economic factors are accounted for, the single biggest incentive to attracting cyber companies and jobs to Indiana will be to outpace other states and regions in the creation of a dynamic and highly educated cybersecurity workforce. If the workforce is supplemented with a rich ecosystem of organically generated start-up companies and public sector opportunities to attract external talent as well, this could represent a long-term growth opportunity for the State.
b. Execution of this growth would require targeted and sustained investment as well as an aggressive campaign to differentiate Indiana's opportunity in comparison to more traditional technology hubs.

**12. What are your communication protocols in a cyber emergency?**

a. The communications sector follows the communication protocols as defined by the Department of Homeland Security and the US-CERT National Cyber Incident Response Plan as documented below.

i. DHS 2015 Sector-specific Plan: https://www.dhs.gov/sites/default/files/publications/nipp-ssp-communications-2015-508.pdf
ii. US-CERT National Cyber Incident Response Plan: https://www.us-cert.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf

b. If a cyber event manifests as or is concurrent with a natural or man-made disaster impacting critical infrastructure, we would additionally follow guidelines associated with the Federal Emergency Management Agency's (FEMA) National Incident Management System (NIMS):
   i. FEMA NIMS FAQ: https://www.fema.gov/pdf/emergency/nims/nimsfaqs.pdf

**13. What best practices should be used across the sectors in Indiana? Please collect and document.**

a. Operationalize knowledge of FEMA's National Incident Management System (NIMS): https://www.fema.gov/pdf/emergency/nims/nimsfaqs.pdf
b. Operationalize the US-CERT National Cyber Incident Response Plan: https://www.us-cert.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf
c. Participate in sector-specific or multi-state Information Sharing Analysis Centers (ISAC): https://www.nationalisacs.org/member-isacs
d. Incorporate threat information sharing technologies, such as STYX/TAXII to move towards machine time as opposed to human time sharing of threat information.
e. Work towards more real-time response technologies and automation to significantly reduce organizational latency in the response to cyberattacks.
f. Invest in cybersecurity awareness training for employees, customers, and your local communities

# Deliverable: Voluntary Industry Contact List

# Deliverable: Voluntary Industry Contact List

## General Information

1. **What is the deliverable?**
    a. Establish Voluntary Industry Contact List

2. **What is the status of this deliverable?**
    a. In-progress; 75% 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. Both the State and other sectors will know who to contact in the associations, companies, and individuals within the Communications Sector, in the event of a cyber incident. Ultimately, the list will help facilitate communication with entities.

6. **What metric or measurement will be used to define success?**
    a. Participation % of companies and individuals to the list

7. **What year will the deliverable be completed?**
    a. While we hope to establish the list in 2018, it will be an ongoing item that will need to be maintained.

8. **Who or what entities will benefit from the deliverable?**
    a. The State and other cybersecurity stakeholders.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. Unknown.

### Additional Questions:

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. None

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. Indiana's Broadband Innovation Group
    b. Indiana Broadband and Technology Association
    c. Satellite Industry Association
    d. Indiana Exchange Carrier Association
    e. Other companies and organizations in the communications sector.

12. **Who should be main lead of this deliverable?**
    a. Joni Hart will work with other stakeholders to gather the appropriate information.

13. **What are the expected challenges to completing this deliverable?**
    a. TBD

## 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 |
|---|---|---|---|---|
| Research Contact Points/Structure | Joni Hart | 95% | 9-26-18 | |
| Design Survey | Joni Hart | 50% | 9-26-18 | |
| Review/Survey Appropriate Housing of Data Collected | Joni Hart | 50% | 9-26-18 | |
| Provide Draft Survey to Sector Members | Joni Hart | 25% | 9-26-18 | |
| Assign Members to assist with subsector response | Joni Hart | 25% | 9-1-18 | |

| | | | | |
|---|---|---|---|---|
| Assign Members to research other state data points | Joni Hart | 25% | 9-1-18 | |
| Survey Response Deadline | Joni Hart | 95% | 9-14-18 | |
| Prepare List for Committee Review | TBA | 0% | 10-1-18 | |
| Finalize Deliverable | TBA | 0% | 10-29-18 | |

## 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 |
|---|---|---|---|---|---|---|
| CSP List | Outreach/ensure participation | $0 | Minimal | - | - | - |

## Benefits and Risks

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

a. The contact lists will facilitate communication between the state and communications sector, and possibly other sectors working with the communications sector.

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

a. Ideally, facilitating communication and reducing time for contact collection during an incident can reduce time and expenses.

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

a. Undeterminable

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

a. Sector participation of 70%

**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. Unknown

**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. TBD

## Other Implementation Factors

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

a. Hesitation for members to contribute data to the state, hesitancy to promote regulation, lack of response, and multi-state contacts for companies.

**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. Administrative support in updating the list.

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

a. Limited

**27. Can this deliverable be used by other sectors?**

a. TBD-will need to assess if members view contacts to be public
b. **If Yes, please list sectors**

## Communications

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

a. TBD-will need to assess if members view contacts to be public

**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

## Evaluation Methodology

**Objective 1:** Develop a form and process to collect a central cyber industry contact list by October 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:** Seventy percent of all communications providers complete annual cyber contact form 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: Communications Sector Terminology Glossary

# Deliverable: Communications Sector Terminology Glossary

## General Information

1. **What is the deliverable?**
    a. Communications Sector Terminology Glossary

2. **What is the status of this deliverable?**
    a. 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. The glossary is intended to provide definition of terminology unique to the communications sector to reduce friction in cross-sector planning and response activities

6. **What metric or measurement will be used to define success?**
    a. Publication of peer-reviewed glossary that removes friction in cross-sector communications regarding cybersecurity incidents.

7. **What year will the deliverable be completed?**
    a. 2018

8. **Who or what entities will benefit from the deliverable?**
    a. All Indiana critical infrastructure sectors can benefit from a better understanding of the communications sector.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. None identified

## Additional Questions

---

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

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. Communications sector entities and industry groups will be consulted in the creation of this glossary.

12. **Who should be main lead of this deliverable?**
    a. Dan Solero

13. **What are the expected challenges to completing this deliverable?**
    a. The communications sector is complex. This complexity will present major challenges in completing a comprehensive and useful document.

## Implementation Plan

---

14. **Is this a one-time deliverable or one that will require sustainability?**
    a. One-time deliverable

## Tactic Timeline

| Tactic | Owner | % Complete | Deadline | Notes |
|---|---|---|---|---|
| Phase 1 questionnaire | Dan Solero | 100 | Feb, 2018 | Complete |
| Phase 2 questionnaire | Dan Solero | 100 | Mar, 2018 | Complete |
| Draft document outline | Dan Solero | 100 | July 1, 2018 | Complete |
| Assign sections to committee members for authorship | Dan Solero | 100 | July 14, 2018 | Complete |
| Review completed first draft document sections for content | Dan Solero | 100 | August 1, 2018 | Complete |
| Revise document based on feedback and edit for flow and grammar | Dan Solero | 100 | August 9, 2018 | Complete |
| Publish release 1 of paper to Syncplicity and IECC website | Dan Solero | 100 | September 2018 | |

## 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 |
|---|---|---|---|---|---|---|
| N/A | | | | | | |

## Benefits and Risks

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

a. The greatest benefit to the glossary is in the reduction of friction related to understanding the complexities and jargon associated with the communications sector. A better understanding of the unique terminology of the communications sector will help with broad planning and execution in the face of chaos associated with a widespread cyberattack.

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

a. This deliverable will not directly reduce risk, but may alleviate impact by facilitating faster, better coordinated, and more robust response from the communications sector

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

a. Without this glossary, the communications sector will likely remain fairly opaque to processes and planning efforts in adjacent sectors.

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

a. Completion and publication of peer-reviewed glossary. (this is a binary metric. Completion and publication = success)

**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. Priorities related to committee member employers and personal commitments may impact timeline, as most members are volunteering their time and effort.

**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. This does not require sustained support.

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

a. Sector-specific associations and private sector companies.

**27. Can this deliverable be used by other sectors?**

a. Yes
   i. IT
   ii. Public Safety

## Communications

---

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

a. Industry associations, MS-ISAC, IN-ISAC, NCC, Comm-ISAC, National Cybersecurity and Communications Integration Center (NCCIC), privately held sector members.

**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. N/A

## Evaluation Methodology

**Objective 1:** Complete Communications Sector Terminology Glossary 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:** Publish Communications Sector Terminology Glossary to IECC website by September 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: Communications Sector Whitepaper

# Deliverable: Communications Sector Whitepaper

## General Information

1. **What is the deliverable?**
    a. Communications Sector Cyber Security Whitepaper

2. **What is the status of this deliverable?**
    a. In-progress; 50% 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. The whitepaper is intended to achieve several objectives, including:
        i. Definition of terminology unique to the communications sector to reduce friction in cross-sector planning and response activities
        ii. Description of typical roles, responsibilities, and incident response practices as well as governing regulations, frameworks, and laws that influence or guide communications sector entities in risk management, threat sharing, operational practice, and incident response
        iii. Mapping and inventory of national, regional, and local entities and services that make up the communications sector in Indiana

6. **What metric or measurement will be used to define success?**
    a. Publication of peer-reviewed whitepaper that facilitates deeper understanding of the communications sector and how its cybersecurity interests are managed and defined

7. **What year will the deliverable be completed?**
    a. 2018

8. **Who or what entities will benefit from the deliverable?**
    a. All Indiana critical infrastructure sectors can benefit from a better understanding of the communications sector.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. None identified

## Additional Questions

---

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

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. Communications sector entities and industry groups will be consulted in creation of this paper.

12. **Who should be main lead of this deliverable?**
    a. Dan Solero

13. **What are the expected challenges to completing this deliverable?**
    a. The communications sector is complex. This complexity will present major challenges in completing a comprehensive and useful document.

## Implementation Plan

---

14. **Is this a one-time deliverable or one that will require sustainability?**
    a. One-time deliverable

## Tactic Timeline

| Tactic | Owner | % Complete | Deadline | Notes |
|---|---|---|---|---|
| Phase 1 questionnaire | Dan Solero | 100 | Feb, 2018 | Complete |
| Phase 2 questionnaire | Dan Solero | 100 | Mar, 2018 | Complete |
| Draft document outline | Dan Solero | 100 | July 1, 2018 | Complete |
| Assign sections to committee members for authorship | Dan Solero | 50 | September 1, 2018 | Sections will be reassigned for completion upon forming the next IECC. |
| Review completed first draft document sections for content | Dan Solero | 0 | September 29, 2018 | May reschedule deadline earlier depending on schedules. |
| Submit reviewed draft document broadly to industry groups, subject matter experts, and peer sectors for comment. | Dan Solero | 0 | September 29, 2018 | This will align to first draft deadline |
| Revise document based on feedback and edit for flow and grammar | Dan Solero | 0 | October 14, 2018 | |
| Publish release 1 of white paper to Syncplicity and IECC web site | Dan Solero | 0 | October 29, 2018 | Dependency on final draft revision schedule. |

## 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 |
|---|---|---|---|---|---|---|
| N/A | | | | | | |

## Benefits and Risks

---

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

a. The greatest benefit to the whitepaper is in reduction of friction related to understanding the complexities and jargon associated with the communications sector. Better understanding of the unique characteristics of the communications sector will help with broad planning and execution in the face of chaos associated with a wide spread cyberattack.

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

a. This deliverable will not directly reduce risk, but may alleviate impact by facilitating faster, better coordinated, and more robust response from the communications sector

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

a. Without this whitepaper, the communications sector will likely remain fairly opaque to processes and planning efforts in adjacent sectors.

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

a. Completion and publication of peer and industry-reviewed whitepaper. (this is a binary metric. Completion and publication = success)
b. Adoption or adaptation of the paper by other jurisdictions or projects. If the paper is well received, other jurisdictions or projects will likely want to use it or adapt it to their use. Baseline is zero, since it does not yet exist. Any adoption or adaptation for use should be viewed as a measure of success.

**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. Priorities related to committee member employers and personal commitments may impact timeline, as most members are volunteering their time and effort.

**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. This does not require sustained support.

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

a. Sector-specific associations and private sector companies.

**27. Can this deliverable be used by other sectors?**

a. Yes
   i. IT
   ii. Public Safety

## Communications

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

a. Industry associations, MS-ISAC, IN-ISAC, NCC, Comm-ISAC, NCCIC, privately held sector members.

**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. N/A

## Evaluation Methodology

**Objective 1:** Complete the Communications Sector Whitepaper for industry by October 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:** Distribute the Communications Sector Whitepaper to eighty percent of identified industry and key stakeholders by November 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 Incident Response Engagement Guide

# Deliverable: Cyber Incident Response Engagement Guidance

## General Information

1. **What is the deliverable?**
    a. Cyber Incident Response Engagement Guidance for Communications Sector

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. The document intends to provide operational guidance on how communications sector principals should be engaged in the event of widespread cyberattack. The resulting action should be faster and more complete engagement of the communications sector in incident response engagements and planning.

6. **What metric or measurement will be used to define success?**
    a. Publication of peer-reviewed and industry-supported engagement guidance document.

7. **What year will the deliverable be completed?**
    a. 2018

8. **Who or what entities will benefit from the deliverable?**
    a. All Indiana critical infrastructure sectors can benefit from a better understanding of the communications sector.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. None identified

## Additional Questions

---

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

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. Communications sector entities and industry groups will be consulted in the creation of this paper.

12. **Who should be main lead of this deliverable?**
    a. Dan Solero

13. **What are the expected challenges to completing this deliverable?**
    a. The communications sector is complex. This complexity will present major challenges in completing comprehensive and useful guidance.

## Implementation Plan

---

14. **Is this a one-time deliverable or one that will require sustainability?**
    a. One-time deliverable

## Tactic Timeline

| Tactic | Owner | % Complete | Deadline | Notes |
|---|---|---|---|---|
| Phase 1 questionnaire | Dan Solero | 100 | Feb, 2018 | Complete |
| Phase 2 questionnaire | Dan Solero | 100 | Mar, 2018 | Complete |
| Research similar engagement guidance documents from adjacent sectors or similar projects | Dan Solero | 0 | September 1, 2018 | Will be assigned at upcoming committee meeting |
| Draft document outline | Dan Solero | 50 | September 1, 2018 | In progress |
| Assign sections to committee members for authorship | Dan Solero | 0 | September 14, 2018 | Will be assigned at upcoming committee meeting |
| Review completed first draft document sections for content | Dan Solero | 0 | September 30, 2018 | May reschedule deadline earlier depending on schedules. |
| Submit reviewed draft document broadly to industry groups, subject matter experts, and peer sectors for comment. | Dan Solero | 0 | October 14, 2018 | This will align to first draft deadline |
| Revise document based on feedback and edit for flow and grammar | Dan Solero | 0 | October 29, 2018 | |
| Publish release 1 of document to Syncplicity | Dan Solero | 0 | November 14, 2018 | Aligned to final draft revision schedule. |

## 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 |
|---|---|---|---|---|---|---|
| N/A | | | | | | |

## Benefits and Risks

---

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

a. The greatest benefit of the whitepaper will be to better facilitate advanced planning and cross-sector alignment around incident response.

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

a. This deliverable will not directly reduce risk, but may alleviate impact by facilitating faster, better coordinated, and more robust response from the communications sector

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

a. Without this document, response coordination may be complicated by needing to research and conduct outreach within the response window. Without the ability to plan ahead, robust response engagement will be extremely challenging.

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

a. Completion and publication of the industry-reviewed document. (this is a binary metric. Completion and publication = success)
b. Approval of the engagement guidance by sector members and industry associations will be an indicator of success.
c. Use of the document or adaptation by similar projects or working groups should also be viewed as a measure of success.

**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. Priorities related to committee member employers and personal commitments may impact timeline, as most members are volunteering their time and effort.
b. Some industry members may have governing regulations that complicate completion of this guidance on schedule.

**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. This does not require sustained support.

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

a. Sector-specific associations and private sector companies.

**27. Can this deliverable be used by other sectors?**

a. Yes
    i. IT
    ii. Public Safety

## Communications

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

a. Industry associations, MS-ISAC, IN-ISAC, NCC, Comm-ISAC, NCCIC, privately held sector members.

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

a. No
    i. The information included in this document may be deemed to disclose operational practices that members do not wish to make available to the public. If at all possible, we would like for the document to be available to the public. This decision will depend on feedback from sector members.

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

a. N/A

## Evaluation Methodology

**Objective 1:** Develop the Communications Sector Engagement Guidance by October 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:** Distribute the Communications Sector Engagement Guidance to eighty percent of identified industry and key stakeholders 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

# 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.

- Telecommunication Terms

# IECC Communications Committee

Telecommunication Terms

August 2018

# Telecommunication Terms

**ACCESS CHARGE**
A fee charged subscribers or other telephone companies by a local exchange carrier for the use of its local exchange networks.

**ADSL**
Asymmetric digital subscriber line (**ADSL**) is a type of digital subscriber line (DSL) technology, a data communications technology that enables faster data transmission over copper telephone lines than a conventional voiceband modem can provide. ADSL differs from the less common symmetric digital subscriber line (SDSL). In ADSL, bandwidth and bit rate are said to be asymmetric, meaning greater toward the customer premises (downstream) than the reverse (upstream). Providers usually market ADSL as a service for consumers for Internet access for primarily downloading content from the Internet, but not serving content accessed by others.

**ANALOG SIGNAL**
A signaling method that uses continuous changes in the amplitude or frequency of a radio transmission to convey information.

**BANDWIDTH**
The width of a communications channel. In analog communications, bandwidth is typically measured in Hertz. In digital communication, bandwidth is measured in bits per second (bps).

**BROADBAND**
In telecommunications, broadband means a wide range of frequencies over which information can be transmitted. A simple way to compare broadband and narrowband Internet connections is to picture a highway. Only one car can travel at a time on a one-lane highway (narrowband). However, when a highway is six or eight lanes wide (broadband), more traffic can drive on the road at the same time.

Think back to when you had a dial-up Internet connection. Now think about the Internet today. You have 'always-on' data connections that enable you to access multiple media sources and a wide range of information at the same time. That's broadband.

**CARRIER**
A company that is authorized by regulatory agencies to operate a telecommunications system. Examples include AT&T, Alltell, and Verizon.

**CDMA (Code Division Multiple Access)**
CDMA is a channel access method used by different radio communication technologies- one way to understand CDMA is to think of a party where everyone is talking at the same time. Lots of confusion, right? CDMA assigns different codes to each group of users, so other groups hear just noise-- and tune out.

**CENTRAL OFFICE (CO)**
In almost every neighborhood there is a windowless building that houses the switching equipment that connects your telephone to your neighbor's telephone or routes your call to another central office for long distance calls. This building is called the central office. The central office has switching equipment that can switch calls locally or to long-distance carrier phone offices.

**CIRCUIT-SWITCHED NETWORK**
Circuit-switched is a type of network in which a physical path is obtained for and dedicated to a single connection between two end-points in the network for the duration of the connection. Ordinary voice phone service is circuit-switched. The telephone company reserves a specific physical path to the number you are calling for the duration of your call. During that time, no one else can use the physical lines involved.

**CLEC - Competitive Local Exchange Carrier**
The Telecommunications Act of 1996 opened the door to competition for local phone service. This act mandated that the Incumbent Local Exchange Carriers (ILEC) such as Verizon, Bell South, or SBC provide the necessary interfaces so that CLECs could provide seamless local service. For example, MegaPath is a CLEC.

**COMMON CARRIER**
In the telecommunications arena, the term used to describe a telephone company.

**COMMUNICATIONS ASSISTANT**
A person who facilitates telephone conversation between text telephone users, users of sign language or individuals with speech disabilities through a Telecommunications Relay Service (TRS). This service allows a person with hearing or speech disabilities to communicate with anyone else via telephone at no additional cost.

**COMMUNITY ANTENNA TELEVISION (CATV)**
A service through which subscribers pay to have local television stations and additional programs brought into their homes from an antenna via a coaxial cable.

**CPE (Customer Provided Equipment)**
Telephone equipment (key systems, PBXs, answering machines, etc.) which live on the customer's premises.

**CSP (Communication Service Provider)**
An umbrella term used to describe both traditional providers of communication services (ie: telecom) and alternate providers such as cable TV companies and other over-the-top providers.

**CSR - Customer Service Record**
A copy of how your telephone records appear in your local carriers' database. It contains information items and charges such as: type of service, federal access charge, number portability charge, calling blocks on the line, 911 charge, etc. It is the "snapshot" of your entire service for each line.

**DAC (Digital Analog Converter)**
A device which converts digital pulses (ie: data) into analog signals so that the signal can be used by analog devices such as phones.

**DC POWER PLANT**
Each Central Office houses an AC power plant as well as an AC/DC converter that runs the majority of the telecommunications equipment. Some Central Office Technicians focus on keeping these power plants running efficiently 24/7.

**DIAL AROUND**
Long distance services that require consumers to dial a long-distance provider's access code (or "10-10" number) before dialing a long-distance number to bypass or "dial around" the consumer's chosen long-distance carrier in order to get a better rate.

**DIGITAL TELEVISION (DTV)**
A new technology for transmitting and receiving broadcast television signals. DTV provides clearer resolution and improved sound quality.

**DIRECT BROADCAST SATELLITE (DBS/DISH)**
A high-powered satellite that transmits or retransmits signals which are intended for direct reception by the public. The signal is transmitted to a small earth station or dish (usually the size of an 18-inch pizza pan) mounted on homes or other buildings.

**DSL (Digital Subscriber Line)**
The technology used between a customer's premises and the telephone company to support the transport of higher bandwidth digital signals on the copper twisted wire pairs already in place as part of the telephony infrastructure. Also known as generic name signifying the family of Digital Subscriber Line technologies including ADSL, HDSL, VDSL, etc.

**DSLAM**
A DSLAM (Digital Subscriber Line Access Multiplexer) is a network device, usually at a telephone company central office, that receives signals from multiple customer Digital Subscriber Line (DSL) connections and puts the signals on a high-speed backbone line using multiplexing techniques. Depending on the product, DSLAM multiplexers connect DSL lines with some combination of asynchronous transfer mode (ATM), frame relay, or Internet Protocol networks. DSLAM enables a phone company to offer business or homes users the fastest phone line technology (DSL) with the fastest backbone network technology (ATM).

**DSO, DS1 & DS3 (Digital Signal 0, 1, 3, etc)**
Different levels of digital hierarchy for the amount and speed of data carried on a circuit. The fundamental speed level is DS-0, which is a voice grade channel.

**DWDM (Dense Wave Division Multiplexing)**
The higher-capacity version of WDM, which is a means of increasing the capacity of fiber-optic data transmission systems through sending many wavelengths of light down a single strand of fiber.

**ENHANCED SERVICE PROVIDERS**
A for-profit business that offers to transmit voice and data messages and simultaneously adds value to the messages it transmits. Examples include telephone answering services, alarm/security companies and transaction processing companies.

**EnodB**
E-UTRAN Node B, also known as Evolved Node B (abbreviated as eNodeB or eNB), is the element in E-UTRA of LTE that is the evolution of the element Node B in UTRA of UMTS. It is the hardware that is connected to the mobile phone network that communicates directly wirelessly with mobile handsets (UEs), like a base transceiver station (BTS) in GSM networks.

Traditionally, a Node B has minimum functionality, and is controlled by a Radio Network Controller (RNC). However, with an eNB, there is no separate controller element. This simplifies the architecture and allows lower response times.

**FTTC, FTTH, FTTB**
Think "Fiber to the ____". In the acronyms above, the ____ is Cabinet, Home and Business and relate to optical fiber extensions. Translation? Access networks that consist of optical fiber from the exchange to the cabinet//home/business.

**FACILITY (facilities)**
A facilities person assigns the cable or fiber pair numbers. The facilities assignment refers to where the telephone number starts in the central office and the route it takes from the central office to the end address (includes those boxes you see on the side of the street).

**FEMTOCELLS**
Femtocells enhance coverage and capacity inside buildings which means fewer dropped calls. This has potential to allow cell phone calls to travel over the internet. *"Femtocells. They will be everyplace. And the cheaper they are, the easier to install. the better coverage you get."* - Ivan Seidenberg, CEO Verizon

**FIBER / FIBER OPTIC CABLE**
Transmits light signals along glass strands, permitting 10-100 times faster transmission than traditional copper wire. What this means to the consumer, is faster, more efficient cell phones and Internet connections.
You may hear FTTH (fiber to the home), FTTP (fiber to the premises). Those terms simply mean – how close the fiber comes to a building, house…end user. The closer it comes, the faster the connection.

**FRAME**
A rack to which telecommunications equipment is mounted. You will see these in Central Offices.

**FRAME RELAY**
The standard for high-speed data communications, offering users transmission speeds of 2.048 megabits per second and higher. It allows faster speeds than the X.25 packet switching standard because it does away with elaborate error-correction and routing information. Its main application is interconnecting local area networks.

**FREQUENCY MODULATION (FM)**
A signaling method that varies the carrier frequency in proportion to the amplitude of the modulating signal.

**GLOBAL POSITIONING SYSTEM (GPS)**
A US satellite system that lets those on the ground, on the water or in the air determine their position with extreme accuracy using GPS receivers.

**HCS (Hierarchical Cell Structure)**
Hierarchical Cell Structure: the architecture of a multi-layered cellular network where subscribers are handed over from the macro to the micro to the pico layer, depending on the current network capacity and the needs of the subscriber.

**HD VOICE**
A technology that provides better audio quality by delivering at least twice the sound range (wideband) of a traditional (narrowband) telephone call.

**HDSL (High Bit Rate Digital Subscriber Line)**
This is digital access technology typically used by businesses. It requires two copper wire pairs (or in some cases fiber) but doesn't require complex engineering and installation.

**HSPA (High Speed Packet Access)**
Often referred to as 3.5G, this is an extension to the original 3G standard providing significantly higher data rates. HSDPA (downlink) can provide theoretical maximum downlink speeds of 168 Mbps. HSUPA (uplink) supports maximum uplink speeds of 22 Mbps.

**INFRASTRUCTURE**
This is an incredibly important part of the communications industry. Roughly 25% of all telecom workers are involved with telecom infrastructure – in its simplest terms, infrastructure includes the pieces and parts that make sophisticated communications systems work.

**INTERACTIVE VIDEO DATA SERVICE (IVDS)**
A communication system, operating over a short distance, that allows nearly instantaneous two-way responses by using a hand-held device at a fixed location. Viewer participation in game shows, distance learning and e-mail on computer networks are examples.

**INSTRUCTIONAL TELEVISION FIXED SERVICE (ITFS)**
A service provided by one or more fixed microwave stations operated by an educational organization and used to transmit instructional information to fixed locations.

**IPTV (Internet Protocol Television)**
Digital television delivered over the Internet. It can be accessed through a closed or public network, with a computer or a set-top box capable of processing the video streams. This is in direct competition with traditional cable and broadcast television. IPTV can be bundled with VoIP and Internet access for a triple play service, increasing the competition that other television providers face.

**ISDN**
**Integrated Services Digital Network** (**ISDN**) is a set of communication standards for simultaneous digital transmission of voice, video, data, and other network services over the traditional circuits of the public switched telephone network. The key feature of ISDN is that it integrates speech and data on the same lines, adding features that were not available in the classic telephone system. The ISDN standards define several kinds of access interfaces, such as Basic Rate Interface (BRI), Primary Rate Interface (PRI), Narrowband ISDN (N-ISDN), and Broadband ISDN (B-ISDN).

ISDN is a circuit-switched telephone network system, which also provides access to packet switched networks, designed to allow digital transmission of voice and data over ordinary telephone copper wires, resulting in potentially better voice quality than an analog phone can provide. It offers circuit-switched connections (for either voice or data), and packet-switched connections (for data), in increments of 64 kilobit/s.

**L2TP (Layer 2 Tunneling Protocol)**
Layer 2 Tunneling Protocol is an IETF (Internet Engineering Task Force) standard tunneling protocol for VPNs. ISPs use this to provide secure, node to node communications in support of multiple, simultaneous tunnels in the core of the internet or IP based networks.

**LANDLINE**
Traditional wired phone service.

**LAND MOBILE SERVICE**
A public or private radio service providing two-way communication, paging and radio signaling on land.

**LATA - Local Access and Transport Area**
Geographic area covered by one or more local telephone companies, which are legally referred to as local exchange carriers (LECs). A connection between two local exchanges within the LATA is referred to as intraLATA. A connection between a carrier in one LATA to a carrier in another LATA is referred to as interLATA. InterLATA is long-distance service. The current rules for permitting a company to provide intraLATA or interLATA service (or both) are based on the Telecommunications Act of 1996.

**LOW POWER FM RADIO (LPFM)**
A broadcast service that permits the licensing of 50-100 watt FM radio stations within a service radius of up to 3.5 miles and 1-10 watt FM radio stations within a service radius of 1 to 2 miles.

**LOW POWER TELEVISION (LPTV)**
A broadcast service that permits program origination, subscription service or both via low powered television translators. LPTV service includes the existing translator service and operates on a secondary basis to regular television stations. Transmitter output is limited to 1,000 watts for normal VHF stations and 100 watts when a VHF operation is on an allocated channel.

**LTE (Long Term Evolution)**
LTE is a broadband access technology that enhances the ability of mobile users to access larger amounts of data. LTE operates on a lower frequency of 700 MHz giving it enhanced signal range and building/obstacle penetration. AT&T and Verizon Wireless are building their 4G networks with LTE technology.

This is a big deal because for the most part, consumers want more and more data. In fact, a recent IBM report shows that when people are asked what they would be least likely to cut back on to save money - people chose mobile phones and broadband Internet only after their homes.

**MICROCELL**
A **microcell** is a cell in a mobile phone network served by a low power cellular base station (tower), covering a limited area such as a mall, a hotel, or a transportation hub. A microcell is usually larger than a picocell, though the distinction is not always clear. A microcell uses power control to limit the radius of its coverage area.

Typically, the range of a microcell is less than two kilometers wide, whereas standard base stations may have ranges of up to 35 kilometers (22 mi). A picocell, on the other hand, is 200 meters or less, and a femtocell is on the order of 10 meters, although AT&T calls its femtocell that has a range of 40 feet (12 m), a "microcell".

**MICROWAVE**
A common form of transmitting telephone and data conversations that occupies a very high frequency range and produces a signal good for about 30 miles.

**MMS (Multimedia Messaging Service)**
The standard in mobile messaging services, adding photos, pictures and audio to text messages.

**MOBILE BROADBAND**
Wireless high-speed internet access through a portable modem, telephone or other device.

**MUST-CARRY (Retransmission)**
A 1992 Cable Act term requiring a cable system to carry signals of both commercial and noncommercial television broadcast stations that are "local" to the area served by the cable system.

**MUX - MULITPLEX**
To transmit two or more signals over a single channel. In the world of CAT5 the explosion of choices that digital TV is bringing the multiplex means to offer subscribers a choice of various starting times for movies and events.

**NETWORK**
A telecommunications network is a collection of terminals, links and nodes which connect together to enable telecommunication between users of the terminals. Networks may use circuit switching or message switching. Each terminal in a network must have a unique address so messages or connections can be routed to the correct one. *Wikipedia definition

**NETWORK OPERATIONS CENTER (NOC)**
A **network operations center** (or **NOC**, pronounced "knock") is one or more locations from which control is exercised over a computer, television broadcast or telecommunications network.

**NUMBER PORTABILITY**
A term used to describe the capability of individuals, businesses and organizations to retain their existing telephone number(s) — and the same quality of service — when switching to a new local service provider.

**OPEN VIDEO SYSTEMS**
An alternative method to provide cable-like video service to subscribers.

**OPERATOR SERVICE PROVIDER (OSP)**
A common carrier that provides services from public phones, including payphones and those in hotels/motels.

**OUTSIDE PLANT**
Refers to all of the physical cabling and supporting infrastructure (such as conduit, cabinets, tower or poles), and any associated hardware (such as repeaters) located between a demarcation point in a switching facility to another switching facility or to a customer premises.

**PACKET SWITCHING**
Packet switching is a method of grouping data which is transmitted over a digital network into *packets* which are made of a header and a payload. Data in the header is used by networking hardware to direct the packet to its destination where the payload is extracted and used by application software. Packet switching is the primary basis for data communications in computer networks worldwide.

**PAGING SYSTEM**
A one-way mobile radio service where a user carries a small, lightweight miniature radio receiver capable of responding to coded signals. These devices, called "pagers," emit an audible signal, vibrate or do both when activated by an incoming message.

**PBX**
Private Branch Exchange Digital or analog telephone switchboard located on the customer premises and used to connect private and public telephone networks.

**PBX (Private Branch Exchange)**
A private (as in owned by the telephone company) exchange (as in the Central Office). A PBX is a small version of the phone company's larger central switching office. In other words, an analog telephone switchboard located on the customer premises and used to connect private and public telephone networks.

**PERSONAL COMMUNICATIONS SERVICE (PCS)**
Any of several types of wireless, voice and/or data communications systems, typically incorporating digital technology. PCS licenses are most often used to provide services similar to advanced cellular mobile or paging services. However, PCS can also be used to provide other wireless communications services, including services that allow people to place and receive communications while away from their home or office, as well as wireless communications to homes, office buildings and other fixed locations.

**PLANT**
A general term for all equipment used by a telephone company to provide telecommunications services. In the telecom business, plant comes in two variations – inside and outside plant. Inside is in a building. Outside is outside the building – on poles, in the ground.

**POTS**
Plain old telephone service (POTS), or plain ordinary telephone service, is a retronym for voice-grade telephone service employing analog signal transmission over copper loops. POTS was the standard service offering from telephone companies from 1876 until 1988 when the Integrated Services Digital Network (ISDN) Basic Rate Interface (BRI) was introduced, followed by cellular telephone systems, and voice over IP (VoIP). POTS remain the basic form of residential and small business service connection to the telephone network in many parts of the world. The term reflects the technology that has been available since the introduction of the public telephone system in the late 19th century, in a form mostly unchanged despite the introduction of Touch-Tone dialing, electronic telephone exchanges and fiber-optic communication into the public switched telephone network (PSTN).

**PRESCRIBED INTEREXCHANGE CHARGE (PICC)**
The charge the local exchange company assesses the long-distance company when a consumer picks it as his or her long-distance carrier.

**PSTN**
The public switched telephone network (PSTN) is the aggregate of the world's circuit-switched telephone networks that are operated by national, regional, or local telephone operators, providing infrastructure and services for public telecommunication. The PSTN consists of telephone lines, fiber optic cables, microwave transmission links, cellular networks, communications satellites, and undersea telephone cables, all interconnected by switching centers, thus allowing most telephones to communicate with each other. Originally a network of fixed-line analog telephone systems, the PSTN is now almost entirely digital in its core network and includes mobile and other networks, as well as fixed telephones.

**RAN**
A **radio access network** (**RAN**) is part of a mobile telecommunication system. It implements a radio access technology. Conceptually, it resides between a device such as a mobile phone, a computer, or any remotely controlled machine and provides connection with its core network (CN). Depending on the standard, mobile phones and other wireless connected devices are varyingly known as user equipment (UE), terminal equipment, mobile station (MS), etc. RAN functionality is typically provided by a silicon chip residing in both the core network as well as the user equipment.

**RBOC (Regional Bell Operating Company)**
There are seven (also known as Baby Bells) which own the local exchange carriers in the US following the divestiture/breakup of AT&T ('Ma Bell') in 1984.

**ROAMING**
The use of a wireless phone outside of the "home" service area defined by a service provider. Higher per-minute rates are usually charged for calls made or received while roaming. Long distance rates and a daily access fee may also apply.

**SS7**
Signaling System No. 7 (SS7) is a set of telephony signaling protocols developed in 1975, which is used to set up and tear down most of the world's public switched telephone network (PSTN) telephone calls. It also performs number translation, local number portability, prepaid billing, Short Message Service (SMS), and other mass market services.

In North America it is often referred to as *CCSS7*, abbreviated for *Common Channel Signaling System 7*. In the United Kingdom, it is called *C7* (CCITT number 7), *number 7* and *CCIS7* (Common Channel Interoffice Signaling 7). In Germany, it is often called ZZK-7 (*Zentraler ZeichengabeKanal Nummer 7*).

**SATELLITE**
A radio relay station that orbits the earth. A complete satellite communications system also includes earth stations that communicate with each other via the satellite. The satellite receives a signal transmitted by an originating earth station and retransmits that signal to the destination earth station(s). Satellites are used to transmit telephone, television and data signals originated by common carriers, broadcasters and distributors of cable TV program material.

**SATELLITE UPLINK**
Uplink refers to a transmission of data in which data flows from a ground-based transmitter to an orbital satellite receiver. Uplink is used to send data to a satellite in Earth’s orbit in order to make changes to the way the satellite functions or simply redirect data to another ground-based receiver. Uplink is used in every application that involves the use of an orbital satellite and is a necessary component of all satellite-based telecommunications systems. Like downlink, uplink depends on the use of C Band, Ku Band, and Ka Band radio frequencies, although the frequency ranges differ in downlink and uplink applications.

**SERVICE PLAN**
The rate plan you select when choosing a wireless phone service. A service plan typically consists of a monthly base rate for access to the system and a fixed amount of minutes per month.

**SERVICE PROVIDER**
A telecommunications provider that owns circuit switching equipment.

**SPLICE**
The joining of two or more cables together by splicing the conductors together. In copper wire telephone cables, splicing is on a mechanical basis and pair-to-pair, with the pairs organized by binder groups and color codes. In optical fiber cables, the splicing is fiber-to-fiber, with the fibers organized by ribbon or colored buffer tube and color code. Fiber optics splicing may be either mechanical splicing or fusion splicing.

**SUBSCRIBER LINE CHARGE (SLC)**
A monthly fee paid by telephone subscribers that is used to compensate the local telephone company for part of the cost of installation and maintenance of the telephone wire, poles and other facilities that link your home to the telephone network. These wires, poles and other facilities are referred to as the "local loop." The SLC is one component of access charges.

**SWITCH - SWITCHING**
A device that channels incoming data from any of multiple input ports to the specific output port that will take the data toward its intended destination. In the traditional circuit-switched telephone network, one or more switches are used to set up a dedicated though temporary connection or circuit for an exchange between two or more parties. On an Ethernet local area network (LAN) a switch determines from the physical device (Media Access Control or MAC) address in each incoming message frame which output port to forward it to and out of. In a wide area packet-switched network such as the Internet, a switch determines from the IP Address in each packet which output port to use for the next part of its trip to the intended destination. * definition from whatis.com

**TARIFF**
The documents filed by a carrier describing their services and the payments to be charged for such services.

**TELECOMMUNICATIONS**
Transmitting signals over a distance in order to communicate. The classic 'tin can' telephone is a very simple telecommunications system. Emerging technologies have brought us far from that model. Today's communication could be via telephone, television, radio, satellite, wireless network, computer network, telemetry, or other means. These technologies, plus many more are converging—you can access the Internet, play videos, or track your children's movements via global positioning system (GPS) technology on your cell phone—so the lines between telecommunications and other industries like computer hardware, application software, consumer electronics and entertainment are getting blurrier all the time.

**TELECOMMUNICATIONS CIRCUIT**
A telecommunication circuit is any line, conductor, or other conduit by which information is transmitted. Originally, this was analog, and was often used by radio stations as a studio/transmitter link (STL) or remote pickup unit (RPU) for their audio, sometimes as a backup to other means. Later lines were digital and used for private corporate data networks.

**TELECOMMUNICATIONS RELAY SERVICE (TRS)**
A free service that enables persons with TTYs, individuals who use sign language and people who have speech disabilities to use telephone services by having a third party transmit and translate the call.

**TELECOMMUNICATIONS SYSTEMS**
Networks of leading-edge technologies such as fiber optic systems, satellites, wireless, telephony, and cable, which are connected to computers that allow organizations and individuals throughout business and industry to communicate instantaneously around the world.

**TELEPHONE EXCHANGE**
A telephone exchange is a telecommunications system used in the public switched telephone network or in large enterprises. An exchange consists of electronic components and in older systems also human operators that interconnect (*switch*) telephone subscriber lines or virtual circuits of digital systems to establish telephone calls between subscribers.

**TELEPHONE LINE**
A telephone line or telephone circuit (or just line or circuit within the industry) is a single-user circuit on a telephone communication system. This is the physical wire or other signaling medium connecting the user's telephone apparatus to the telecommunications network, and usually also implies a single telephone number for billing purposes reserved for that user. Telephone lines are used to deliver landline telephone service and Digital subscriber line (DSL) phone cable service to the premises. Telephone overhead lines are connected to the public switched telephone network.

**TELEPHONE NUMBER**
A telephone number is a sequence of digits assigned to a fixed-line telephone subscriber station connected to a telephone line or to a wireless electronic telephony device, such as a radio telephone or a mobile telephone, or to other devices for data transmission via the public switched telephone network (PSTN) or other private networks.

**TELEPHONY**
The word used to describe the science of transmitting voice over a telecommunications network.

**TIRKS (Trunks Integrated Record Keeping System)**
An operations support system developed by the Bell System during the late 1970s. It was developed for inventory and order control management of interoffice trunk circuits that interconnect telephone switches. It grew to encompass and automate many functions required to build the ever-expanding data transport network. Supporting circuits from POTS and 150 baud modems up through T1, DS3, SONET and DWDM, it continues to evolve today, and unlike many software technologies today, provides complete backward compatibility. TIRKS is in use at AT&T, Verizon, CenturyLink, and Cincinnati Bell Telephone.

**TOLL**
A device that receives calls and allows them to be transmitted to the next local calling area, thus avoiding toll or access charges.

**TRUNK / TRUNKING**
A communication line between two switching systems. The term switching system typically includes equipment in a Central Office and PBXs. A tie trunk connects PBXs. Central office trunks connect a PBX to the switching system at the Central Office.

**TTY**
A type of machine that allows people with hearing or speech disabilities to communicate over the phone using a keyboard and a viewing screen. It is sometimes called a TDD.

**TWISTED CABLE PAIR**
Twisted pair cabling is a type of wiring in which two conductors of a single circuit are twisted together for the purposes of improving electromagnetic compatibility. Compared to a single conductor or an untwisted balanced pair, a twisted pair reduces electromagnetic radiation, crosstalk between neighboring pairs and improves rejection of external electromagnetic interference. It was invented by Alexander Graham Bell.

**UNIVERSAL SERVICE**
The financial mechanism which helps compensate telephone companies or other communications entities for providing access to telecommunications services at reasonable and affordable rates throughout the country, including rural, insular and high costs areas, and to public institutions. Companies, not consumers, are required by law to contribute to this fund. The law does not prohibit companies from passing this charge on to customers.

**VDSL**
Very-high-bit-rate digital subscriber line (VDSL) and very-high-bit-rate digital subscriber line 2 (VDSL2) are digital subscriber line (DSL) technologies providing data transmission faster than asymmetric digital subscriber line (ADSL).

VDSL offers speeds of up to 52 Mbit/s downstream and 16 Mbit/s upstream, over a single flat untwisted or twisted pair of copper wires using the frequency band from 25 kHz to 12 MHz. These rates mean that VDSL is capable of supporting applications such as high-definition television, as well as telephone services (voice over IP) and general Internet access, over a single connection. VDSL is deployed over existing wiring used for analog telephone service and lower-speed DSL connections

**VIDEO HEADEND**
The Video Headend is the point in the network which linear (e.g., broadcast TV) and on-demand (e.g., movies) content is captured and formatted for distribution over a network. The headend ingests national feeds of linear programming via satellite either directly from the broadcaster or programmer or via an aggregator. The Headend takes each individual channel and allows the operator the option to use RF or encode it into digital video format, like Mpeg 2 or Mpeg 4, for both standard (SD) and high definition (HD) television signals. This digital video formatted content is then ingested into a Quam or IP network for delivery.

**VIVID**
The acronym VIVID includes each component of the evolving communications industry: Voice, Information, Video, Infrastructure & Data. Check out our Industry Overview page to see some of the vivid components of telecom in action.

**VOICE**
Audible communication over a traditional land-line, wireless cellular or smart phone or even through a computer via VOIP.

**VOIP (Voice over Internet Protocol)**
Harnesses the power of broadband internet connections to allow consumers access to telephone services over the internet. In other words, your words get converted into data signals and travel over the internet. Once they get to their destination, they are converted from data signals back into analog signals and transmitted. Upgrades in technology helped combat problems with early VoIP, such as poor quality and availability of service. Today's VoIP is a viable competitor to traditional telephony. As businesses continue to cut costs and limit travel budgets, expect to see the use of VoIP increase.

**VoLTE**
VoLTE, or Voice Over LTE is similar to VoIP- but goes one step further. Instead of using the hardware at the ends of the call (the phones), VoLTE offloads the heavy lifting to the network- creating VoIP HD. Beyond a crisp and clear sound, VoLTE includes the ability to cancel echos and background noise on the back end, not the handset itself *.
*definition taken from pocketnow.com

**WIDE AREA NETWORK (WAN)**
A computer or communications network that covers a geographic area which is larger than a business campus. Usually, the dividing line between a local or campus network and an Wide Area Network is a router. On the local or campus side, the transmission lines in a network (copper or fiber) are usually owned by the enterprise. On the WAN side, the lines are typically owned by a carrier and leased to an enterprise.
By far, the most familiar – and largest WAN is the Internet.

**WIRELESS**
Wireless telecommunications carriers provide telephone, Internet, data, and other services to customers through the transmission of signals over networks of radio towers. The signals are transmitted through an antenna directly to customers, who use devices, such as cell phones and mobile computers, to receive, interpret, and send information.

**3G and 4G**
These terms refer to third- and fourth-generation cellular wireless capabilities. 3G and 4G networks allow mobile and smart phone users to access more information and services on their devices faster. It's because of these technological advances that you can video chat, watch Internet TV, play online games, download videos and listen to streaming music on your phone. Simply put, 3G and 4G allow you to do more.

Both 3G and 4G—now enhanced by LTE technology—are available across most of the U.S. today. The major difference between the two is speed. In general, 4G LTE networks are much faster than 3G LTE networks.

**5G**

Fifth-generation wireless, or 5G, is the latest iteration of cellular technology, engineered to greatly increase the speed and responsiveness of wireless networks. With 5G, data transmitted over wireless broadband connections could travel at rates as high as 20 Gbps by some estimates -- exceeding wireline network speeds -- as well as offer latency of 1 ms or lower for uses that require real-time feedback. 5G will also enable a sharp increase in the amount of data transmitted over wireless systems due to more available bandwidth and advanced antenna technology.