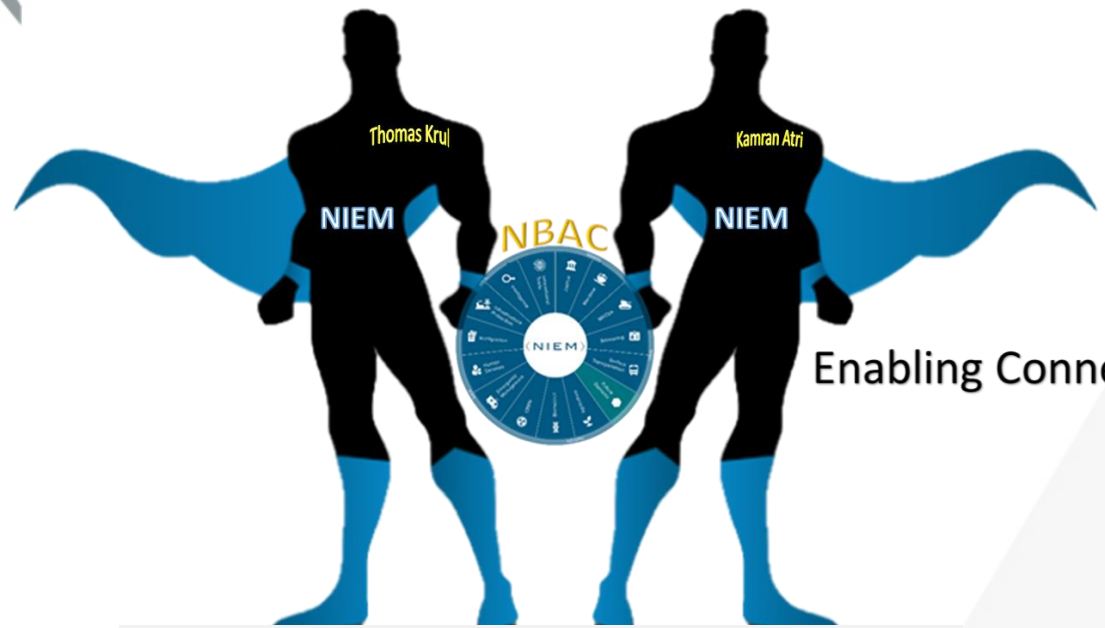
NIEM NBAC F2F 2021

Session III - NIEM Stewardship

NIEM™



Enabling Connected ~~Future~~ Now

SESSION III – NIEM STEWARDSHIP

NBAC ANNUAL MEETING - DAY 2			
NBAC Annual Meeting (Wednesday, 15 September 2021) AM Session			
Location: Virtual - MS TEAMS			
Time (EDT)	**Subject**	**Speaker (s)/ Facilitator(s)**	**Description**
10 -10:05	Introduction/Agenda	NBAC Co-Chairs (Mr. Kamran Atri & Mr. Thomas Krul)	• Welcome • Agenda
10:05 - 10:40	Keynote Speaker	Ms. Stacy Wright (Cybercrime Support Network, VP of Cyber Resiliency Services)	• What are the data sharing impacts as it relates to Cyber? • Best Practices for implementing Cyber data Standards?
10:40 - 10:50	Session Introduction	Mr. Thomas Krul	• NIEM Stewardship
10:50 - 11	Break		
11 - 11:50	**Session III - NIEM Stewardship**	Mr. Thomas Krul	• Domain Stewardship "Best Practices" • Domain Testimonial/s
11:50 - 12	QA/Wrap-up/Action items	NBAC Co-Chairs (Mr. Kamran Atri & Mr. Thomas Krul)	• Closing

HOUSEKEEPING:

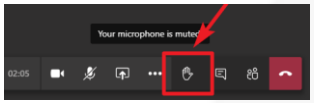
- ***MUTE your mic when you're not talking***
- ***Identify yourself before you start to speak***
- ***Speak clearly***
- ***Disable "call waiting" feature***
  (the clicking noise can be heard by all)

Please note: All 2021 sessions are audio recorded for NIEM training & communications purposes

QUESTIONS & ANSWERS ARE ENCOURAGED!

To signal you want to contribute without interrupting the speaker
- Enter comments via **CHAT window** at any time

To signal a question or respond to a question
- Click on '**Raise your hand**' button on meeting toolbar



(Lower hand after you've talked by clicking hand button again)

All session briefings are available on **NIEM's GitHub** for download as they occur

https://github.com/NIEM/NIEM-Annual-Meetings/tree/master/2021

Session Speakers

- Primary Facilitator
  - Thomas Krul

Public Safety Canada
publicsafety.gc.ca

- Primary Facilitator
  - Kamran Atri

A4SAFE

- Keynote Speaker
  - Stacy Wright

Cybercrime SUPPORT NETWORK

REMINDER:

- *Every NBAC member shares and is part of NIEM decision-making process.*
- *We will seek consensus for decisions arising from the NBAC F2F 2021.*
- *The TEAMS meeting (s) will be recorded, action items assigned, and decisions implemented.*
- *We plan to adhere to the topics and schedule as outlined in the Agenda.*
- *Don't be shy, speak up when you have something to say.*
- *Ask questions if you are unclear or unsure… share your views.*
- *Expand your professional network here with your fellow data standards gurus.*

NIEM STEWARDSHIP

- ***The Domain Steward represents a Community of Interest (COI) comprised of participants across International, Federal, State, Local, and Tribal organizations, components, and agencies.***

- ***The importance of the Steward (and those who work with them)***
  - ***Govern and maintain (responsibilities)***

- ***But we also need them to:***
  - ***Evangelize the Domain***
  - ***Keep it fresh, keep it evergreen***
  - ***Search for opportunities***
  - ***Search for partners***
  - ***Mentorship program***

STEWARDSHIP CHALLENGES

- ***Domains are not artefacts, they are alive, they grow.***

- ***Challenge factors:***
  - ***Maturity***
  - ***Lack of innovation***
  - ***Fear of change***
  - ***Participation in tiger teams***

STACY WRIGHT

Stacey A. Wright, CISSP, is the Vice President of Cyber Resiliency Services at the non-profit Cybercrime Support Network (CSN) where she supports CSN's mission to assist individuals and small businesses before, during, and after a cybercrime incident.

Stacey leads projects to assist the U.S. Cybersecurity and Infrastructure Security Agency (CISA) in developing the Cyber domain for the National Information Exchange Model (NIEM) and the development of the international Cyber Classification Compendium.

She works with multiple partners and stakeholders around the world, particularly in state and local governments, and law enforcement.

Previously, Stacey was the Directors of Partnerships and Cyber Intelligence at the Multi-State Information Sharing and Analysis Center (MS-ISAC) at the Center for Internet Security (CIS), where she developed partnerships and produced timely, actionable, unbiased state, local, tribal, and territorial government and elections-focused insight.

In addition, Stacey teaches a graduate cybersecurity and threat intelligence course at the State University of New York. Prior to her employment at CIS, Stacey was the Cyber Intelligence Analyst for the Federal Bureau of Investigation (FBI) Albany Division, where she was responsible for coordinating the local cyber intelligence program and served as the FBI's liaison to the MS-ISAC. Stacey began her career as an Information Systems Specialist for the Cambridge, MA, Public Safety departments. She received her Bachelor of Science in Criminal Justice from Northeastern University and her Master of Business Administration from the University of Massachusetts, Boston.

She is a formally trained Intelligence Analyst and a national speaker on cybercrime.

Issues, Challenges, and Pitfalls in the Cyber Domain

Ms. Stacey Wright
Cybercrime Support Network
VP of Cyber Resiliency Services

AGENDA

- Cybercrime Support Network
- Unique Data Sharing Issues in Cyber
- Information Sharing Pitfalls
- Best Practices in Implementing Data Standards
- Challenges of Emerging Technology

Cybercrime Support Network

Cybercrime Support Network (CSN) is a national nonprofit whose mission is to serve individuals and small businesses impacted by cybercrime.

Report. ❯ Recover. ❯ Reinforce.

The Problem

Finding resources

Lack of reporting

Law enforcement & 9-1-1 do not have tools

Finding the criminal is hard

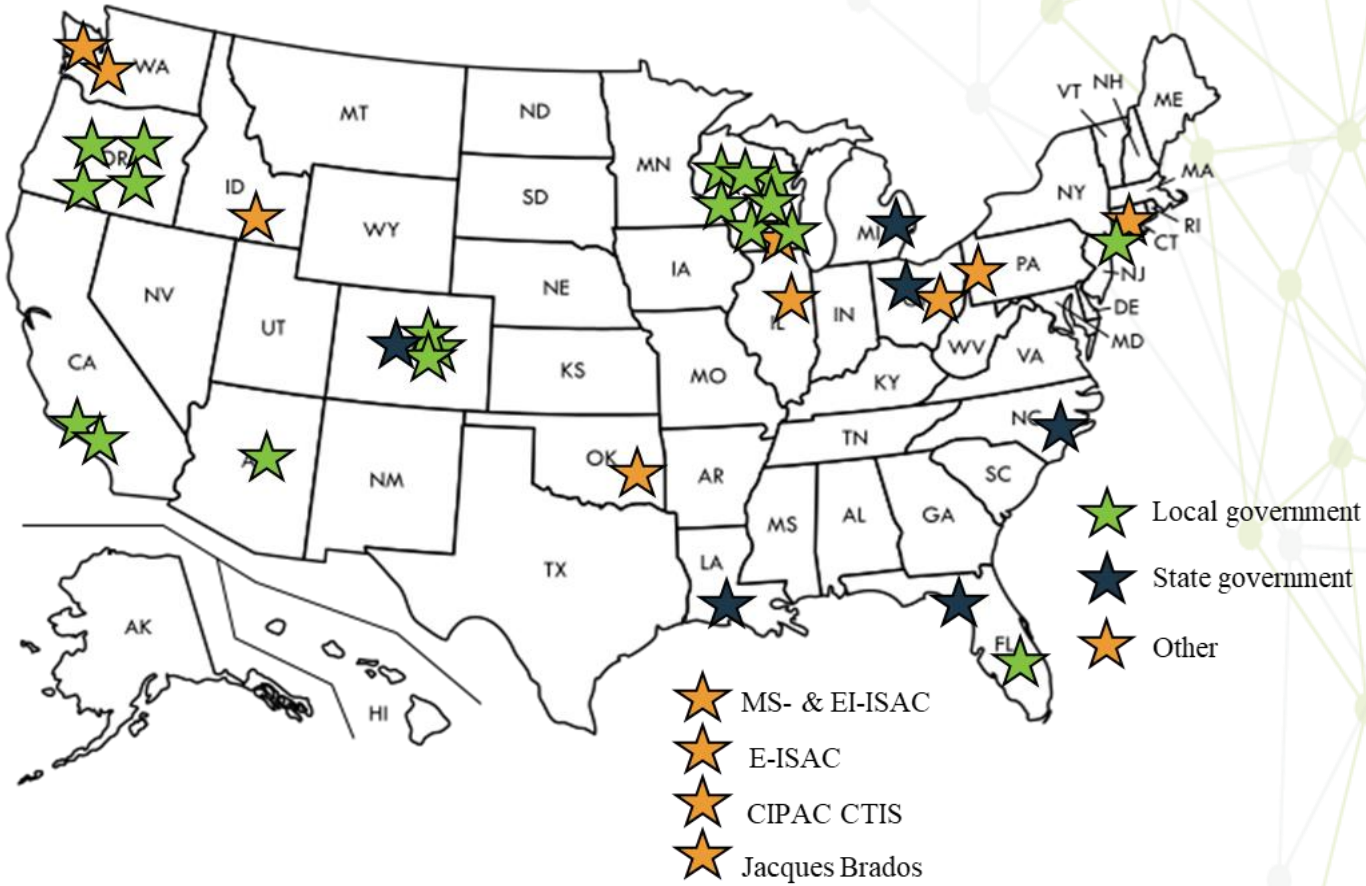
What does success look like?

- Increased reporting
- Increased recovery
- Increased resources
- **Decreased crime and re-victimization**

CSN Is Helping Build the NIEM Cyber Domain

- CSN was awarded a cooperative agreement from the Cybersecurity & Infrastructure Security Agency (CISA) to develop a State, Local, Tribal & Territorial (SLTT) NIEM Cyber Pilot
- We are working with partners to extend the NIEM Cyber Doma
- Goals are to…
  - Ensure the Cyber domain meets the needs of SLTT agencies
  - Encourage NIEM adoption among SLTT agencies
  - Create sets of Information Exchange Package Documentation (IEPDs) used to facilitate information exchange
  - Pilot the Cyber domain among SLTT agencies
- Our focus is on incident response and cyber physical systems

SLTT Stakeholders: 38



TLP:GREEN

Unique Data Sharing Issues in Cyber

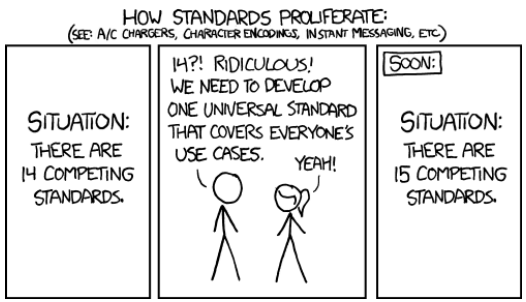
- Compliance driver requirements don't match each other
- Different purposes have led to different taxonomies and terms
- Different maturity levels

Compliance Drivers Don’t Match

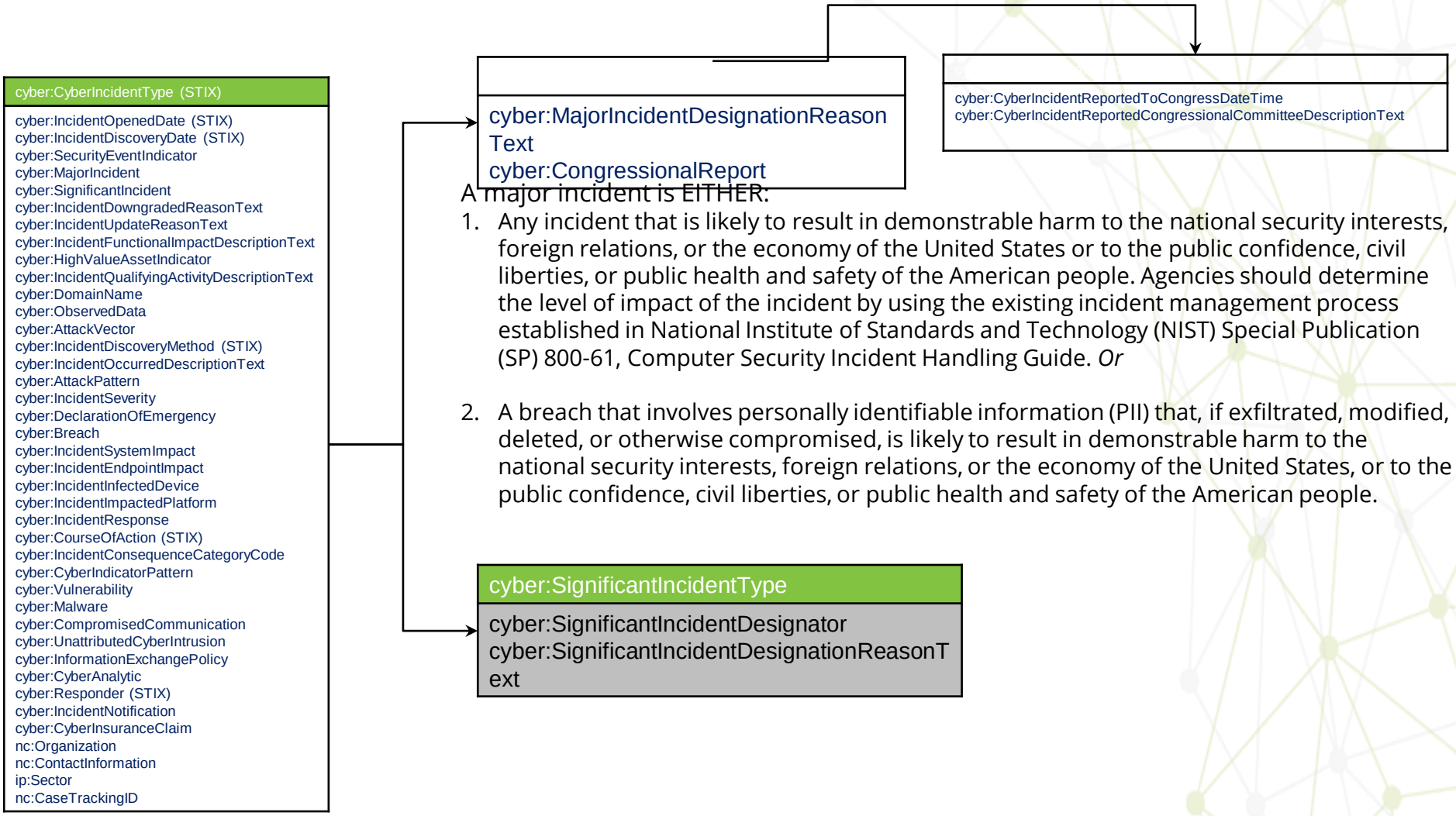
- Protected Critical Infrastructure Information (PCII)
- Federal Tax Information (FTI) under IRS1075
- Personal Health Information (PHI)/electronic PHI (ePHI)
- Federal Trade Commission’s (FTC) Health Breach Notification Rule.
- FTC collects Children's Online Privacy Protection Act (COPPA)
- Family Educational Rights and Privacy Act (FERPA)
- Criminal Justice Information System (CJIS) and information incidents
- Federal Energy Regulatory Commission (FERC)
- North American Electricity Reliability Corporation (NERC)
- ISACs, such as the Elections Infrastructure ISAC, Electricity ISAC, Health ISAC, Multi-State ISAC, and WaterISAC, and information sharing organizations, such as TribalNet
- Payment Card Industry (PCI) Data Security Standard (DSS)
- Local laws and regulations:
  - California Consumer Privacy Act (CCPA)
  - California Civil Code s. 1798.29(a) requires state agencies to disclose data breaches affecting unencrypted PII
  - Louisiana Cyber Incident Response Plan, Emergency Support Function 17 (ESF17)

Different Taxonomies

- **Ad hoc** – self developed taxonomies and ontologies
- **STIX / TAXII**
  - Structured Threat Information Expression (STIX™) is a language and serialization format used to exchange cyber threat intelligence (CTI).
  - Trusted Automated Exchange of Intelligence Information (TAXII™) is an application layer protocol for the communication of cyber threat information in a simple and scalable manner.
- **VERIS Framework**
  - Vocabulary for Event Recording and Incident Sharing (VERIS) is a set of metrics designed to provide a common language for describing security incidents in a structured and repeatable manner.



Different Terms



A major incident is EITHER:

1. Any incident that is likely to result in demonstrable harm to the national security interests, foreign relations, or the economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people. Agencies should determine the level of impact of the incident by using the existing incident management process established in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-61, Computer Security Incident Handling Guide. *Or*

2. A breach that involves personally identifiable information (PII) that, if exfiltrated, modified, deleted, or otherwise compromised, is likely to result in demonstrable harm to the national security interests, foreign relations, or the economy of the United States, or to the public confidence, civil liberties, or public health and safety of the American people.

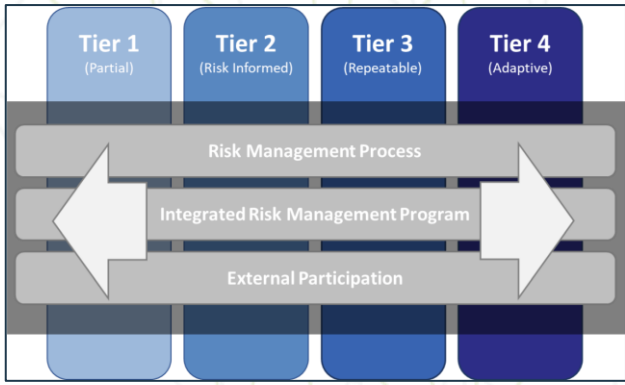
Different Maturity Levels

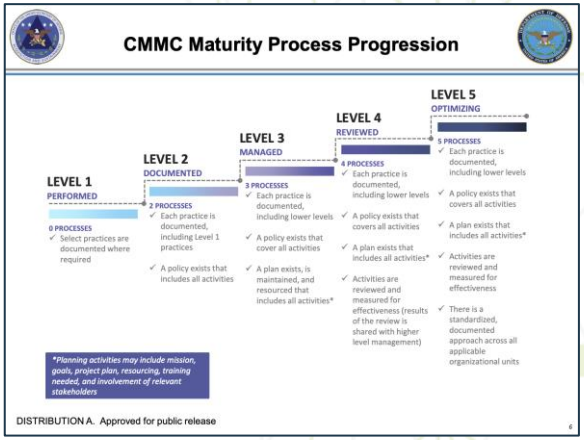
"Some small orgs even ask 'what are IOCs' [tactical intel] and 'what do I do with them?'"

-SLTT NIEM Stakeholder

Capability to Send and Receive Information

Maturity Level		Sending Agency		
		Lower	Medium	Mature
Receiving Agency	Lower	Tactical	Tactical, ~~Operational~~	Tactical, ~~Operational,~~ ~~Strategic~~
	Medium	Tactical	Tactical, Operational	Tactical, Operational, ~~Strategic~~
	Mature	Tactical	Tactical, Operational	Tactical, Operational, Strategic





Information Sharing Pitfalls

- Cyber incidents are not cyber crimes
- POET (Political, Operational, Economic, and Technical)
- Information sharing varies by network design, cardinality, and restrictions

Cyber Incidents ≠ Cyber Crimes

"There's often an unhelpful conceptual distinction between 'cyber incidents' vs. 'cyber crimes.' [The lack of s]haring is still bad for both, but especially rare if there is no perceived loss or harm to a company that could constitute a crime. This is a missed opportunity since 'cyber incidents' including attempted crime/penetrations can still provide valuable insights for the larger cybersecurity community."

-SLTT NIEM Stakeholder

Approaches to Cybercrime	Cyber-enabled crime	Cyber-native (dependent) crime
Malicious cyber activity	Doxing someone; Identifying targets for home robberies via social media; Using online street maps to plan a bank robbery	Writing malware code; Scanning a network for vulnerabilities or open ports; Failed credential stuffing attempts
Illegal cyber activity	Identity theft through misconfigured and exposed databases	Computer/network access and trespass (AKA intrusions); Malware deployment

Political, Operational, Economic, and Technical

cyber:CyberIncidentType (STIX)

- cyber:IncidentOpenedDate (STIX)
- cyber:IncidentDiscoveryDate (STIX)
- cyber:SecurityEventIndicator
- cyber:MajorIncident
- cyber:SignificantIncident
- cyber:IncidentDowngradedReasonText
- cyber:IncidentUpdateReasonText
- cyber:IncidentFunctionalImpactDescriptionText
- cyber:HighValueAssetIndicator
- cyber:IncidentQualifyingActivityDescriptionText
- cyber:DomainName
- cyber:ObservedData
- cyber:AttackVector
- cyber:IncidentDiscoveryMethod (STIX)
- cyber:IncidentOccurredDescriptionText
- cyber:AttackPattern
- cyber:IncidentSeverity
- cyber:DeclarationOfEmergency
- cyber:Breach
- cyber:IncidentSystemImpact
- cyber:IncidentEndpointImpact
- cyber:IncidentInfectedDevice
- cyber:IncidentImpactedPlatform
- cyber:IncidentResponse
- cyber:CourseOfAction (STIX)
- cyber:IncidentConsequenceCategoryCode
- cyber:CyberIndicatorPattern
- cyber:Vulnerability
- cyber:Malware
- cyber:CompromisedCommunication
- cyber:UnattributedCyberIntrusion
- cyber:InformationExchangePolicy
- cyber:CyberAnalytic
- cyber:Responder (STIX)
- cyber:IncidentNotification
- cyber:CyberInsuranceClaim
- nc:Organization
- nc:ContactInformation
- ip:Sector
- nc:CaseTrackingID

cyber:DeclarationOfEmergencyType

- cyber:DeclarationOfEmergencyDesignator
- cyber:ResourceDeploymentReasonText
- nc:StartDate
- nc:EndDate

solarwinds

2020 hack

Software Bill of Materials (SBOM)

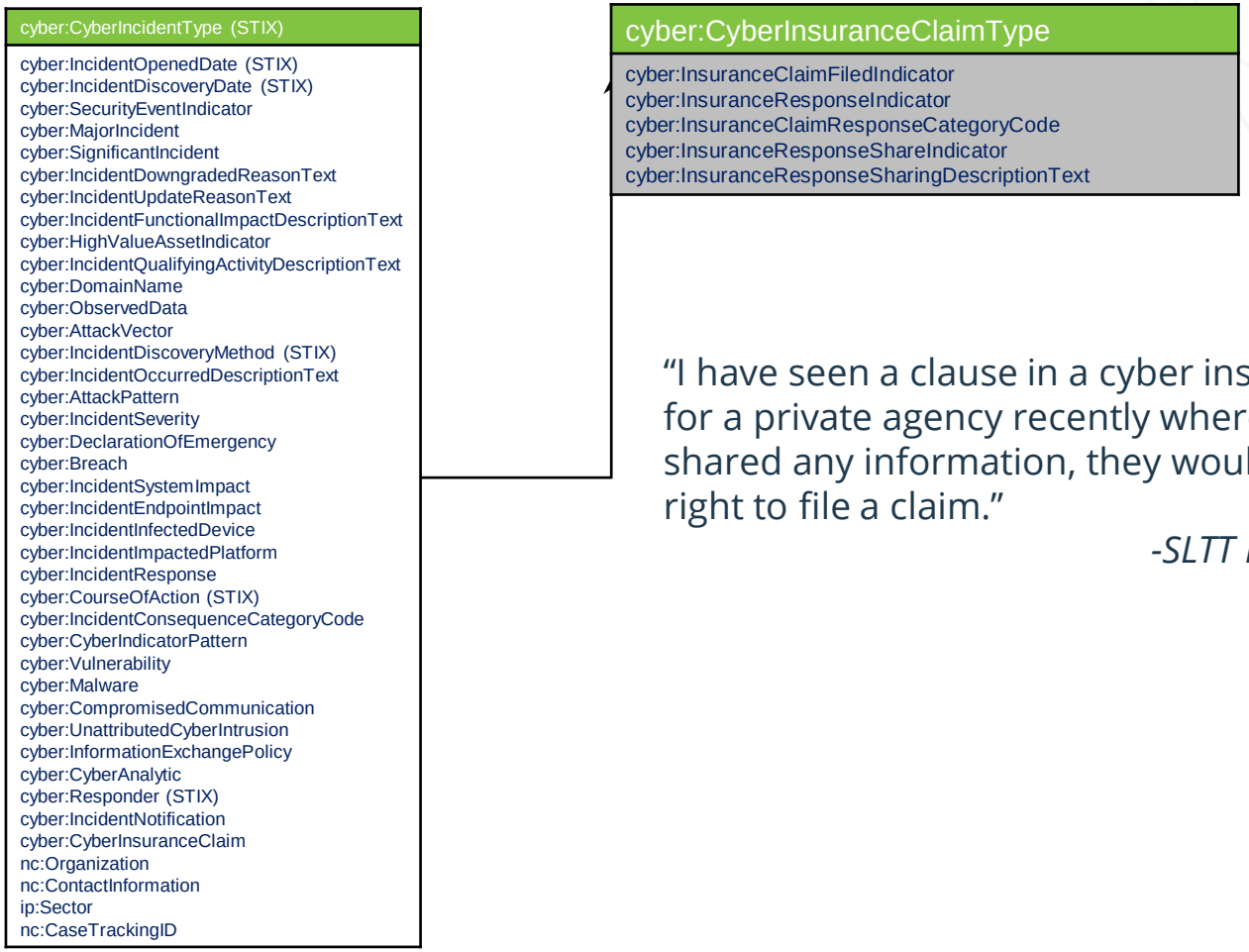
Executive Order on Improving the Nation's Cybersecurity, May 12, 2021

Sec. 4. Enhancing Software Supply Chain Security

(e) Within 90 days of publication of the preliminary guidelines pursuant to subsection (c) of this section, the Secretary of Commerce acting through the Director of NIST, in consultation with the heads of such agencies as the Director of NIST deems appropriate, shall issue guidance identifying practices that enhance the security of the software supply chain.

(vii) providing a purchaser a Software Bill of Materials (SBOM) for each product directly or by publishing it on a public website;

Political, Operational, Economic, and Technical



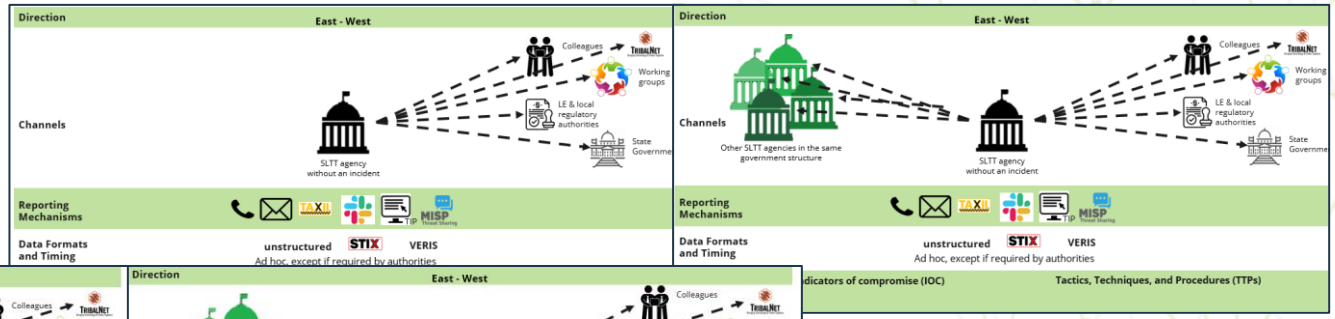
"I have seen a clause in a cyber insurance contract for a private agency recently where if the agency shared any information, they would forfeit the right to file a claim."

-SLTT NIEM Stakeholder

Network Design & Cardinality

Network Types:

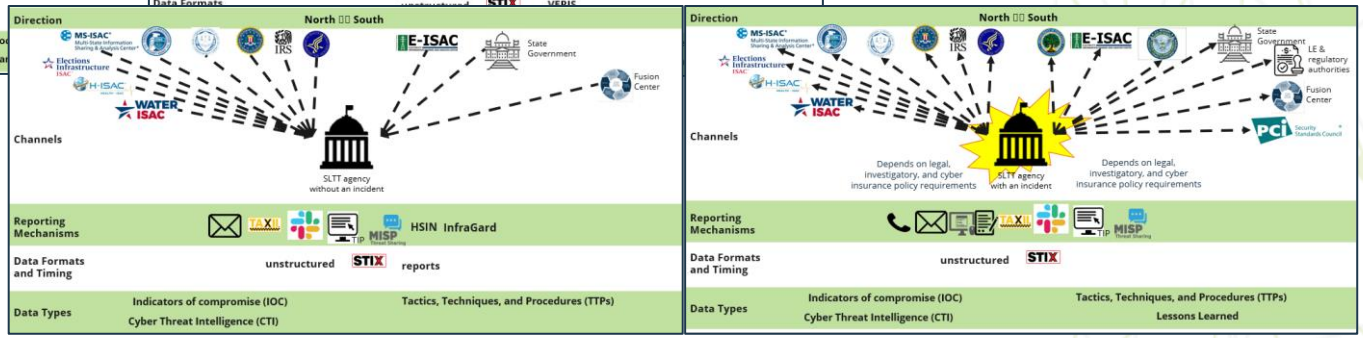
- Centralized
- Decentralized
- Distributed



With an incident is different than without an incident

Compliance Drivers:

- Federal Government
- SLTT Government
- Private Industry



Best Practices in Implementing Data Standards

- Existing data standards, schemas, frameworks, and other considerations
- Security and privacy are key

Existing Data Standards, Schemas, Frameworks, Considerations…

- Anti-Phishing Working Group (APWG) proposed schema for expressing sharing designations
- Common Attack Pattern Enumeration and Classification (CAPEC)
- Common Configuration Enumeration (CCE)
- Common Configuration Scoring System CCSS Specification
- Common Platform Enumeration (CPE)
- Common Vulnerability Enumeration (CVE)
- Common Vulnerability Reporting Framework (CVRF)
- Common Vulnerability Scoring System (CVSS)
- Common Weakness Scoring System (CWSS™)
- Common Weakness Enumeration (CWE™)
- Common Weakness Risk Analysis Framework (CWRAF™)
- Cybersecurity Information Exchange Framework (CYBEX)
- DMTF (formerly known as the Distributed Management Task Force) Common Information Model (CIM).
- FIRST Information Exchange Policy (IEP).
- Internet Engineering Task Force (IETF) Resource-Oriented Lightweight Information Exchange (ROLIE)
- Incident Object Description Exchange Format (IODEF) [RFC 5070]
- IETF's Managed Incident Lightweight Exchange (MILE)
- Knowledge Discovery Metamodel (KDM)
- Malware Attribute Enumeration and Characterization (MAEC)
- Malware Information Sharing and Threat Intelligence Sharing Platform (MISP)
- NIST's Asset Summary Reporting (ASR)
- OASIS Open Cybersecurity Alliance (OCA)
- OASIS Application Vulnerability Description Language (AVDL)
- Open Security Controls Assessment Language (OSCAL)
- Open Vulnerability and Assessment Language (OVAL®).
- Open Checklist Interactive Language (OCIL)
- OpenIOC
- Policy Language for Assessment Results Reporting (PLARR)
- Real-time Inter-network Defense (RID) (IETF/RFC)
- Transport of Real-time Inter-network Defense (RID-T) Messages (IETF/RFC)
- Software Identification (SWID) Specification (ISO 19770-2)
- Structured Threat Information Expression (STIX™)/Trusted Automated Exchange of Intelligence Information (TAXII™)
- Security Content Automation Protocol (SCAP)
- Assessment Results Format (ARF)
- ARF Structured Assurance Case Metamodel (SACM) Specification (OMG)
- VERIS (vocabulary for event recording and incident sharing)
- eXtensible Configuration Checklist Description Format (XCCDF)

Security and Privacy

cyber:CyberIncidentType (STIX)

cyber:IncidentOpenedDate (STIX)
cyber:IncidentDiscoveryDate (STIX)
cyber:SecurityEventIndicator
cyber:MajorIncident
cyber:SignificantIncident
cyber:IncidentDowngradedReasonText
cyber:IncidentUpdateReasonText
cyber:IncidentFunctionalImpactDescriptionText
cyber:HighValueAssetIndicator
cyber:IncidentQualifyingActivityDescriptionText
cyber:DomainName
cyber:ObservedData
cyber:AttackVector
cyber:IncidentDiscoveryMethod (STIX)
cyber:IncidentOccurredDescriptionText
cyber:AttackPattern
cyber:IncidentSeverity
cyber:DeclarationOfEmergency
cyber:Breach
cyber:IncidentSystemImpact
cyber:IncidentEndpointImpact
cyber:IncidentInfectedDevice
cyber:IncidentImpactedPlatform
cyber:IncidentResponse
cyber:CourseOfAction (STIX)
cyber:IncidentConsequenceCategoryCode
cyber:CyberIndicatorPattern
cyber:Vulnerability
cyber:Malware
cyber:CompromisedCommunication
cyber:UnattributedCyberIntrusion
cyber:InformationExchangePolicy
cyber:CyberAnalytic
cyber:Responder (STIX)
cyber:IncidentNotification
cyber:CyberInsuranceClaim
nc:Organization
nc:ContactInformation
ip:Sector
nc:CaseTrackingID

cyber:CyberIndicatorType (STIX)

cyber:CyberIndicatorName (STIX)
cyber:CyberIndicatorDescriptionText (STIX)
cyber:CyberIndicatorDefensiveMeasureText
cyber:CyberIndicatorDefensiveMeasureComplianceIndicator
cyber:KillChainPhase
cyber:TrafficLightProtocolCode
cyber:CyberIndicatorDiamondModelClassificationCode

Color	When should it be used?	How may it be shared?
TLP:RED Not for disclosure, restricted to participants only.	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.
TLP:AMBER Limited disclosure, restricted to participants' organizations.	Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.**
TLP:GREEN Limited disclosure, restricted to the community.	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.
TLP:WHITE Disclosure is not limited.	Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Challenges of Emerging Technology

- Rapid evolution of technology
- Rapid evolution of crime

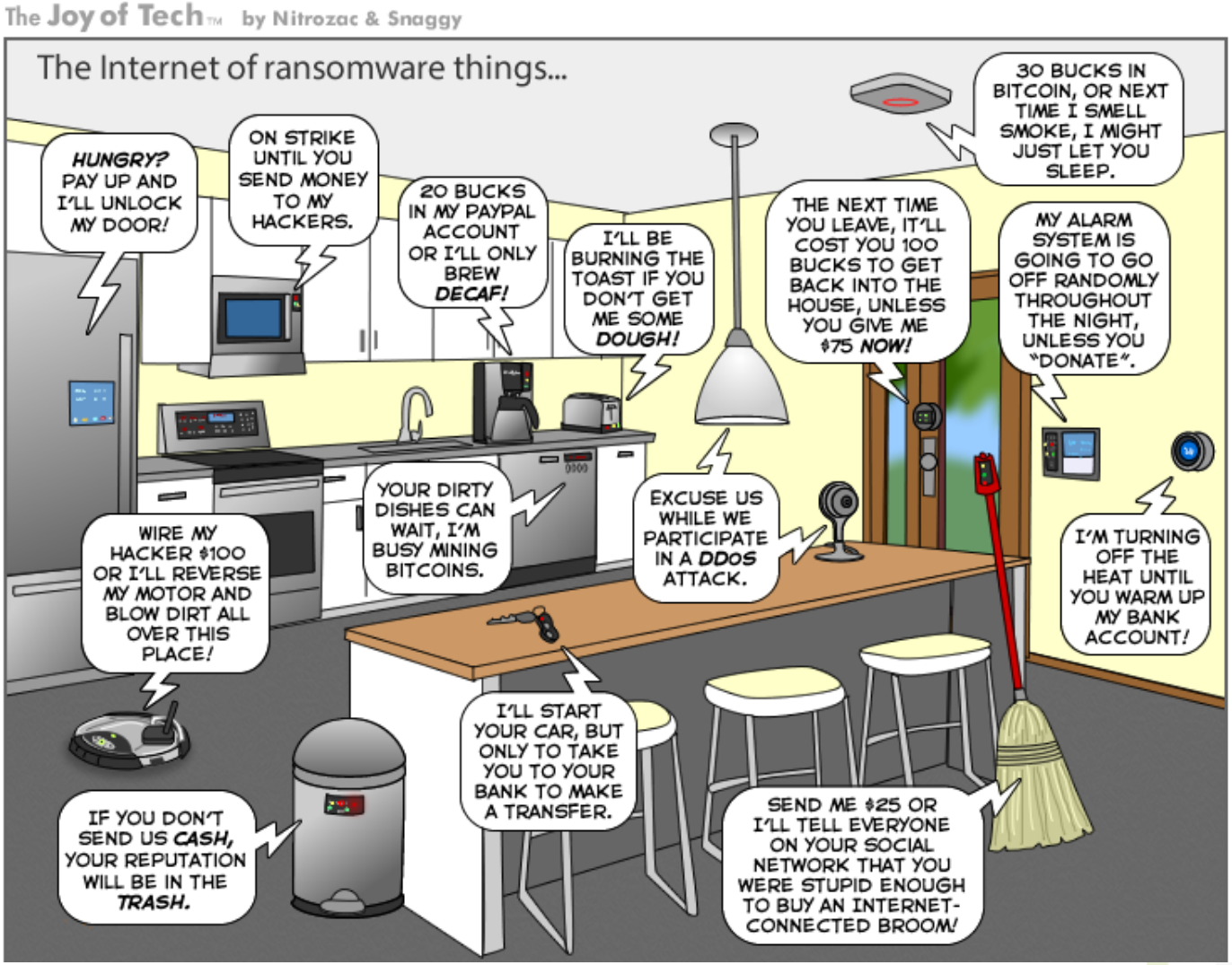
Rapid Evolution of Technology

The Unknown
As we know,
There are known knowns.
There are things we know we know.
We also know
There are known unknowns.
That is to say
We know there are some things
We do not know.
But there are also unknown unknowns,
The ones we don't know
We don't know.

— Donald H. Rumsfeld, Secretary of Defense
Feb. 12, 2002, Department of Defense news briefing

"Nice, but as long as there are readers there will be scrolls."

Rapid Evolution of Crime



NIEM SLTT CPS Scope

Sector	Priority 1 CPS 1. known cyber incidents involve these devices to significant effect, or 2. compliance drivers mandate knowledge	Priority 2 CPS 1. known cyber incidents involve these devices to limited effect, or 2. high potential for targeting with high integration in SLTTs	Priority 3 CPS 1. Medium potential for targeting with at least medium integration in SLTTs and theoretical incident affects	Not Included 1. known or theoretical cyber incidents involve these devices to minimal or no effect, or 2. Low priority for targeting, or 3. Low integration in SLTTs
Communications		Reverse 9-1-1 systems/IPAWS related	Public access network	Smart speakers
Dams	Chemical concentration sensors; Hydroelectric power sensors, controllers		Water level sensors	
Emergency Services Sector	Emergency sirens	UAVs	Fingerprint machines in PDs	License plate readers (LPRs), Gunshot detectors
Energy	Electricity generation and distribution sensors, actuators, controllers, SCADAs, HMIs, and other ICS		Vehicle charging stations; Fuel pumps	
Financial Services	POS systems	ATMs; Gaming machines; Money counters	Tax return scanners; check printers	Parking meters
Government Facilities	HVACs; Door locks/badging/access control systems; Voting machines; Ballot readers/ tabulators	Smart parking meters; Cameras; Elevators	Light system; Fire sensing and suppression systems	Bed bug monitors; Hotel reservation integration system
Healthcare and Public Health	Medical pumps	Defibrillators; Imaging systems; Lab equipment	Refrigeration temperature monitor; Pharmacy robot arms	Wearable health devices (e.g., Fitbit)
Transportation Systems	Pass readers (metros); Self-driving cars	Toll systems; Traffic lights; Air entry/air exit systems; Digital license plates	Vehicle sensors; Air ground traffic automation	
Water and Wastewater	Chemical sensors; Fluid and solid valve controllers; Pump controllers; SCADAs, HMIs, and other ICS		Water meters	

Thank You!

- Stacey Wright
  - SWright@cybercrimesupport.org
- Ilene Klein
  - ilene@cybercrimesupport.org
- David Wagner
  - davidw@cybercrimesupport.org

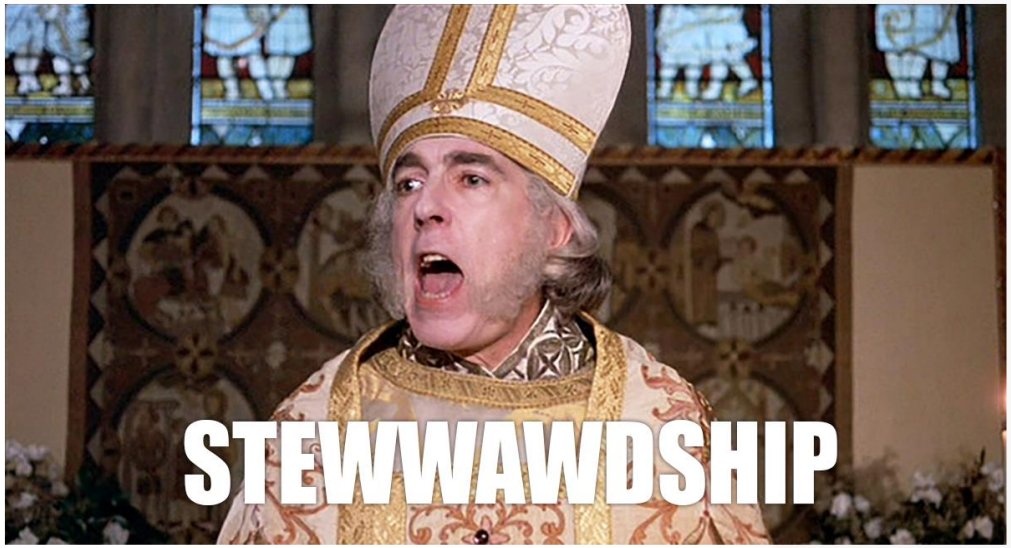
Cybercrimesupport.org
FraudSupport.org
ScamSpotter.org

YouTube:
Cybercrime Support Network

Twitter:
@FraudSupport
@CyberSupportNet

STEWARDSHIP

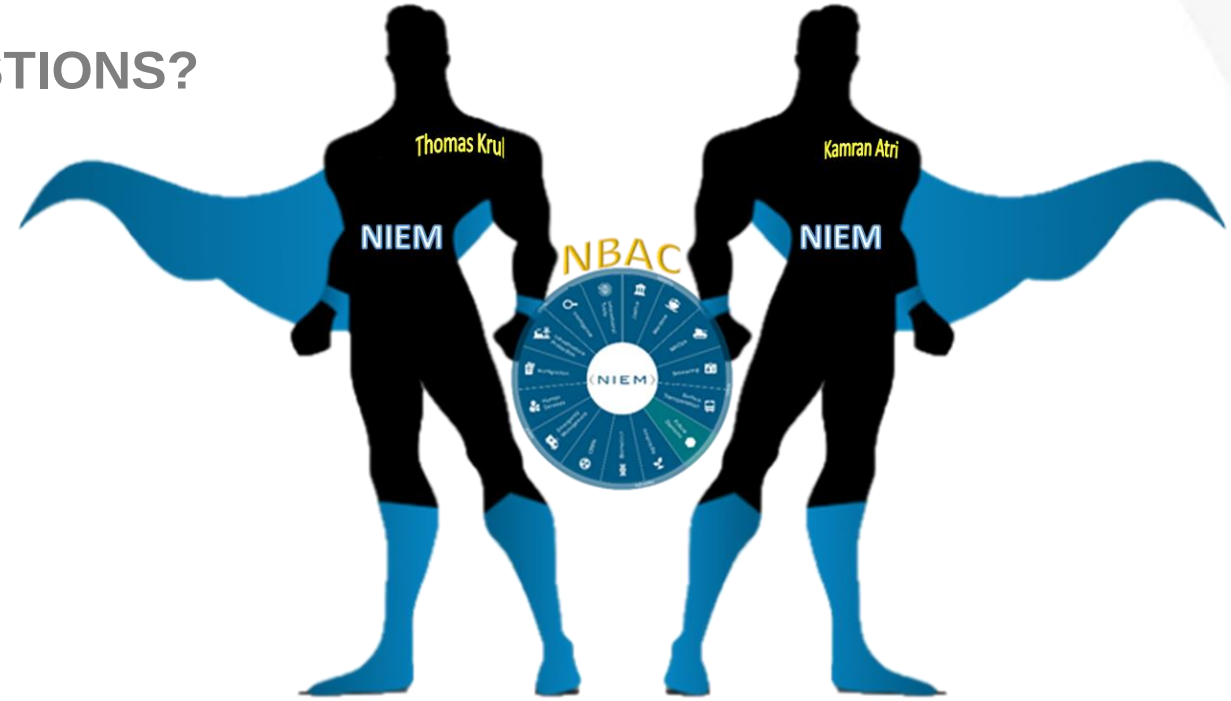
- ***Review***
- ***Improve***
- ***Help that Growth & Outreach grow and reach out***



- ***NIEM Plays a Key Role in:***
  - Designating an Organization as a " **Data Driven Organization** ".
  - Organizations that must Consume, Access, Manipulate, Manage, Analyze, Standardize, Share and Distribute all Available Data from Existing or New Potential Data Sources.
  - Data Architecture, Data Management and Data Engineering, the Key Components of any IT Modernization Life Cycle.

Enabling Connected ~~Future~~ Now

QUESTIONS?



- Thomas Krul — Public Safety Canada (publicsafety.gc.ca)

thomas.krul@canada.ca

NBAC Co-Chairs

- Kamran Atri — A4SAFE

katri@A4SAFE.COM

NBAC Co-Chairs

- Stephen M. Sullivan — Booz | Allen | Hamilton

Stephen.m.sullivan14.ctr@mail.mil
Sullivan_Stephen@bah.com

NBAC Secretariat –NIM PMO

NEXT NIEM F2F SESSION IV – IMPORTANCE OF TRAINING

NBAC ANNUAL MEETING - DAY 2			
NBAC Annual Meeting (Wednesday, 15 September 2021) **PM Session**			
Location: Virtual - MS TEAMS			
1 - 1:05	Introduction/Agenda	NBAC Co-Chairs (Mr. Kamran Atri & Mr. Thomas Krul)	• Welcome • Agenda
1:05 - 1:30	Guest Speakers	Mr. Paul Wormeli & Mr. Michael Phillips (SLTT Co-Chairs)	• NIEM State, Local, Tribal & Territorial Tiger Team "Best Practices & Training"
1:30 - 1: 50	Session Introduction	Mr. Kamran Atri	
1:50 - 2	Break		
2:00 - 2:50	**Session IV - NIEM Importance of Training** Guest Speaker	Mr. Kamran Atri Mr. Michel Savoie (Employment and Social Development / Government of Canada (ESDC)) & Ms. Tsegenet Telda (ESDC)	• Importance of Training • IEPD Steps for Project Discovery & Development • Information sharing impacting data to day operations • What are some of the information sharing pitfalls?
2:50 - 3	Q&A/Wrap-up/Action Items	NBAC Co-Chairs (Mr. Kamran Atri & Mr. Thomas Krul)	• Closing