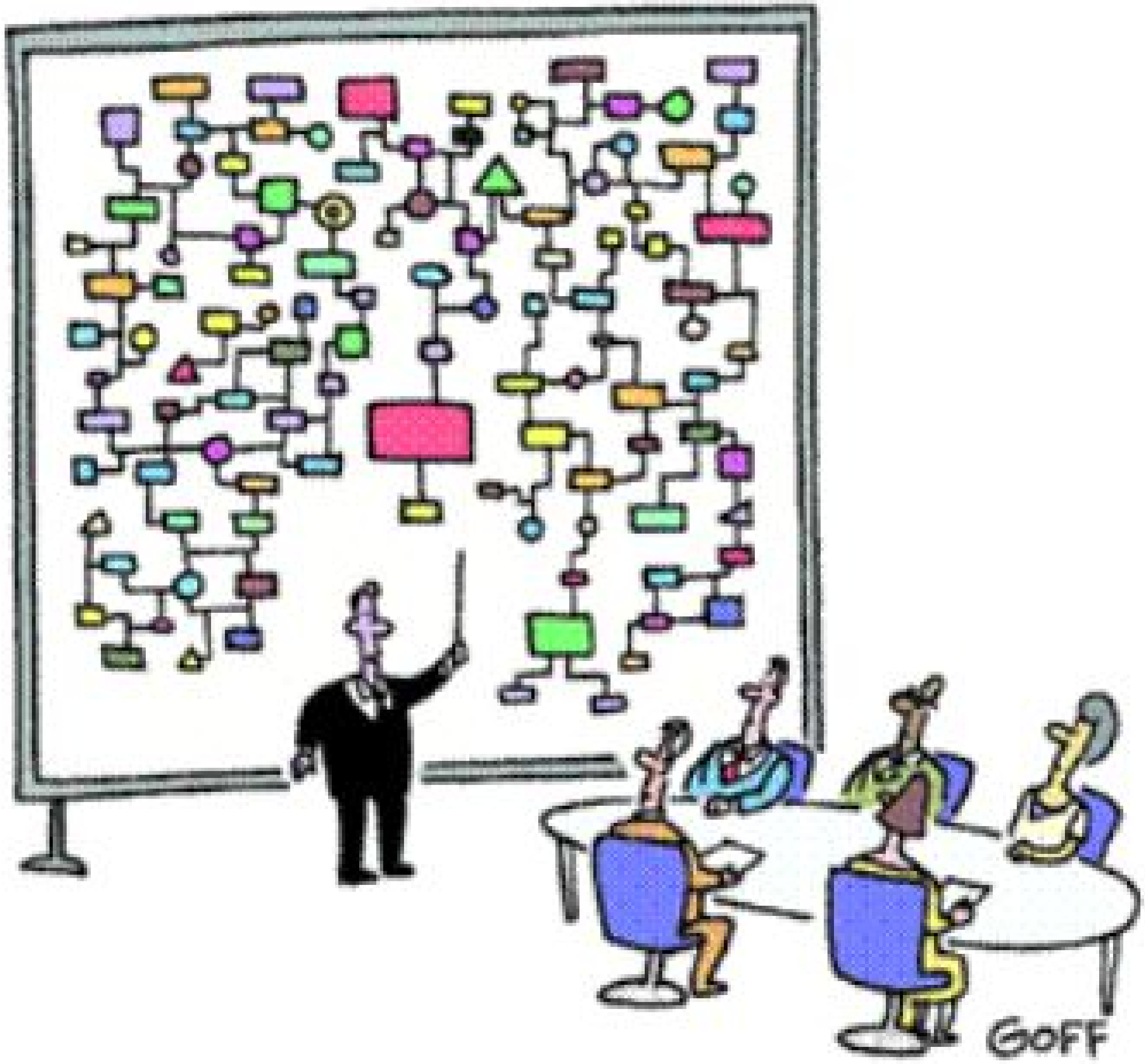
Critical Infrastructure Threat Information Sharing Framework

Briefing to National Association of Regulatory Utility Commissioners

February 12, 2017

U.S. Department of Homeland Security

Homeland Security



"And that's why we need a ~~computer.~~" Framework

…Because I’m a Government Employee

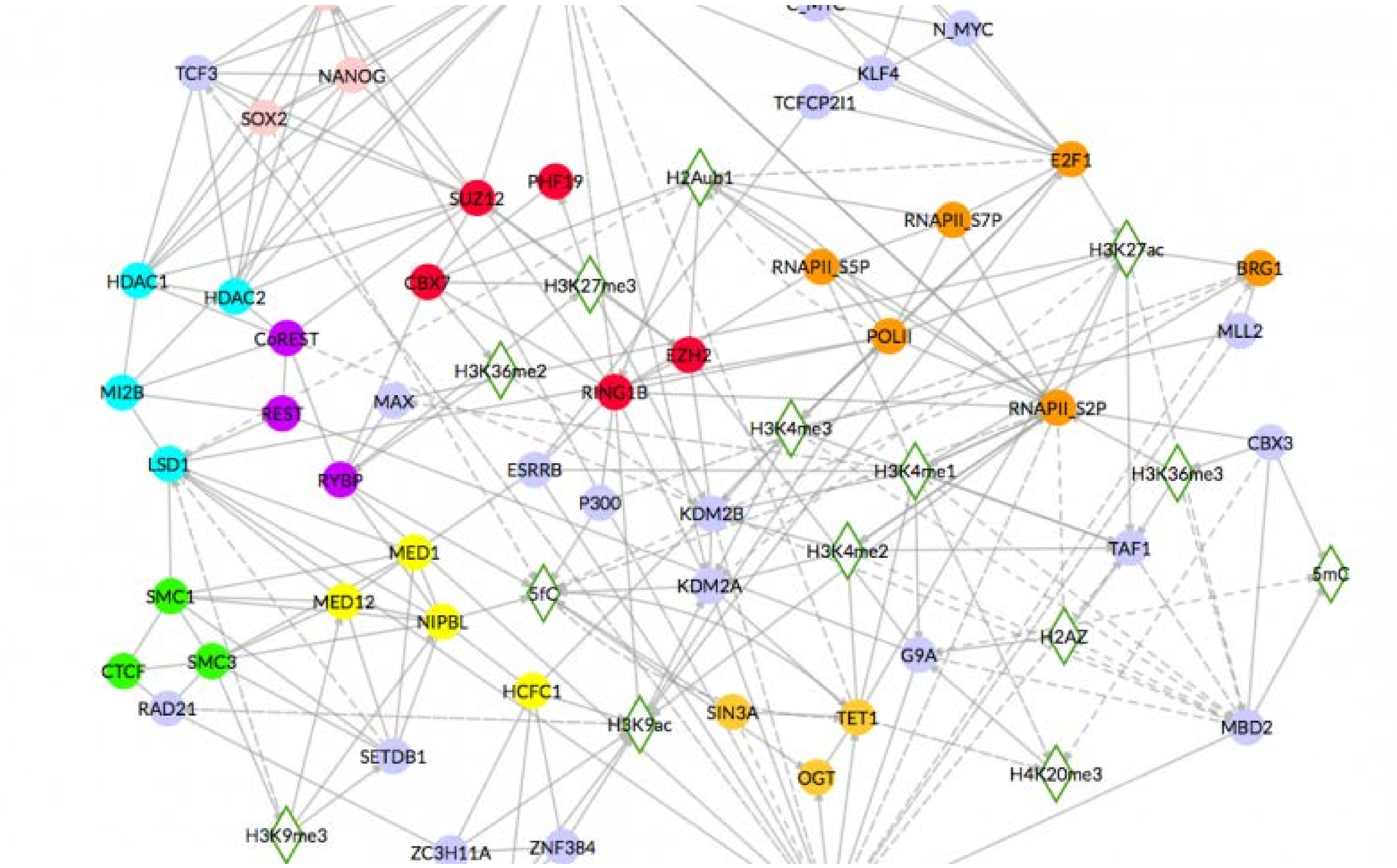
Guidance Documents

- National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience
  - “Share actionable and relevant information across the critical infrastructure community to build awareness and enable risk-informed decision making”
- National Strategy for Information Sharing and Safeguarding

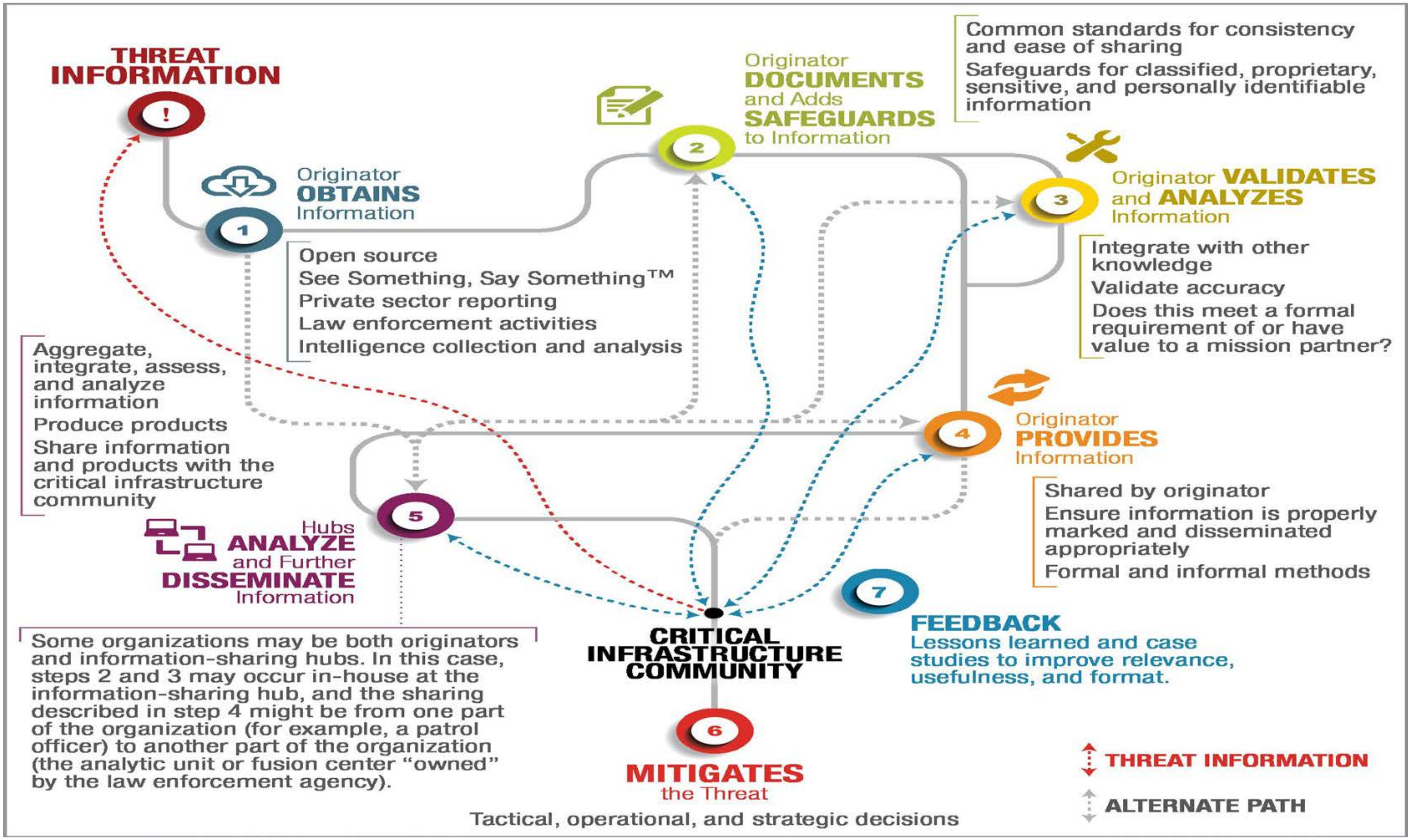
Purpose and Scope

- “…describe the current processes used to facilitate the flow of threat information between and among all entities involved in the critical infrastructure security and resilience mission, and provide an overview of the key threat information-sharing entities which facilitate this process.”
- “…limited to threat information sharing pertaining to manmade threats, including both cyber and physical threats, to critical infrastructure.”

Approach


N_MYC
TCF3
NANOG
KLF4
TCFCP2I1
SOX2
E2F1
PHF19
H2Aub1
SUZ12
RNAPII_S7P
H3K27ac
RNAPII_S5P
BRG1
HDAC1
CBX7
H3K27me3
HDAC2
MLL2
CoREST
POLII
EZH2
H3K36me2
MI2B
MAX
RING1B
REST
RNAPII_S2P
H3K4me3
CBX3
LSD1
ESRRB
H3K4me1
H3K36me3
RYBP
P300
KDM2B
TAF1
H3K4me2
MED1
5fC
5mC
KDM2A
SMC1
MED12
NIPBL
H2AZ
G9A
CTCF
SMC3
HCFC1
SIN3A
TET1
RAD21
H3K9ac
MBD2
SETDB1
OGT
H4K20me3
H3K9me3
ZC3H11A
ZNF384

How Threat Information Sharing Is Done



THREAT INFORMATION

Originator **OBTAINS** Information

- Open source
- See Something, Say Something™
- Private sector reporting
- Law enforcement activities
- Intelligence collection and analysis

Originator **DOCUMENTS** and Adds **SAFEGUARDS** to Information

- Common standards for consistency and ease of sharing
- Safeguards for classified, proprietary, sensitive, and personally identifiable information

Originator **VALIDATES** and **ANALYZES** Information

- Integrate with other knowledge
- Validate accuracy
- Does this meet a formal requirement of or have value to a mission partner?

Originator **PROVIDES** Information

- Shared by originator
- Ensure information is properly marked and disseminated appropriately
- Formal and informal methods

Hubs **ANALYZE** and Further **DISSEMINATE** Information

- Aggregate, integrate, assess, and analyze information
- Produce products
- Share information and products with the critical infrastructure community

Some organizations may be both originators and information-sharing hubs. In this case, steps 2 and 3 may occur in-house at the information-sharing hub, and the sharing described in step 4 might be from one part of the organization (for example, a patrol officer) to another part of the organization (the analytic unit or fusion center "owned" by the law enforcement agency).

CRITICAL INFRASTRUCTURE COMMUNITY

MITIGATES the Threat

Tactical, operational, and strategic decisions

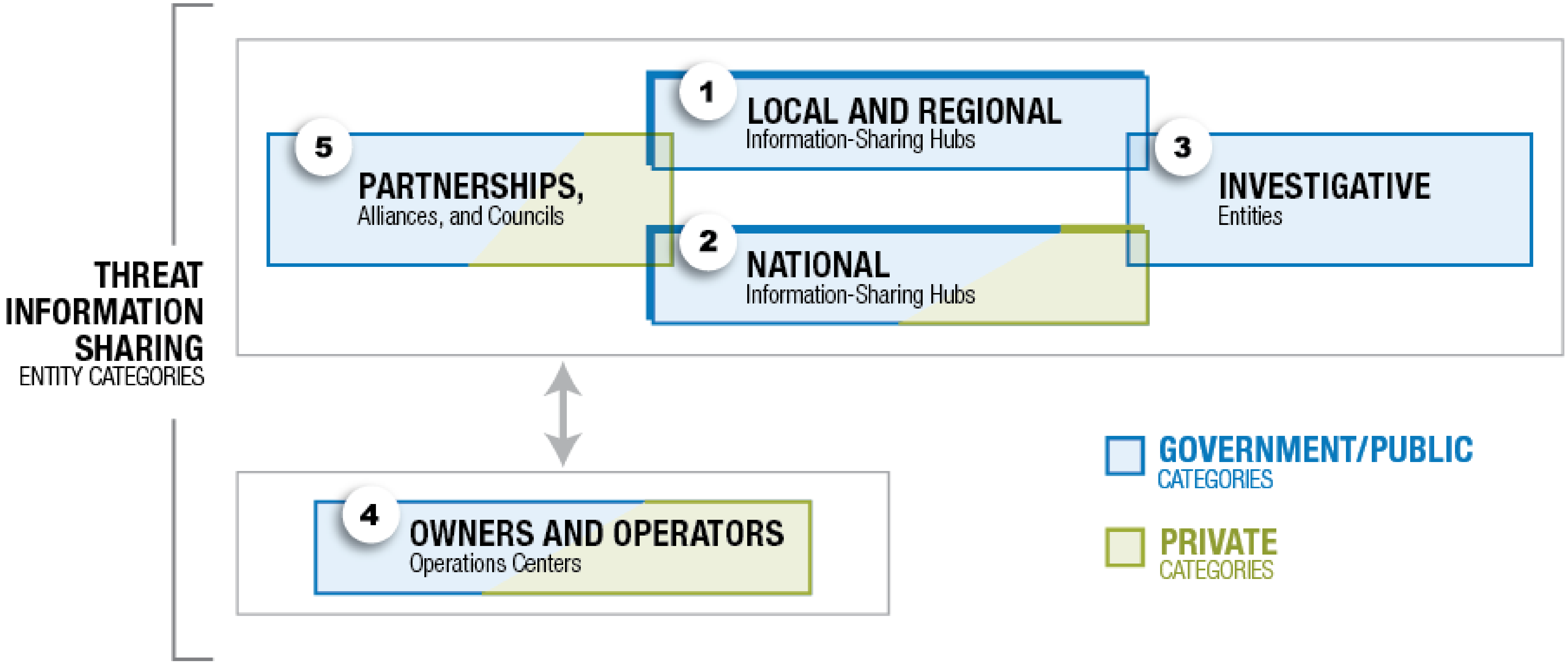
FEEDBACK

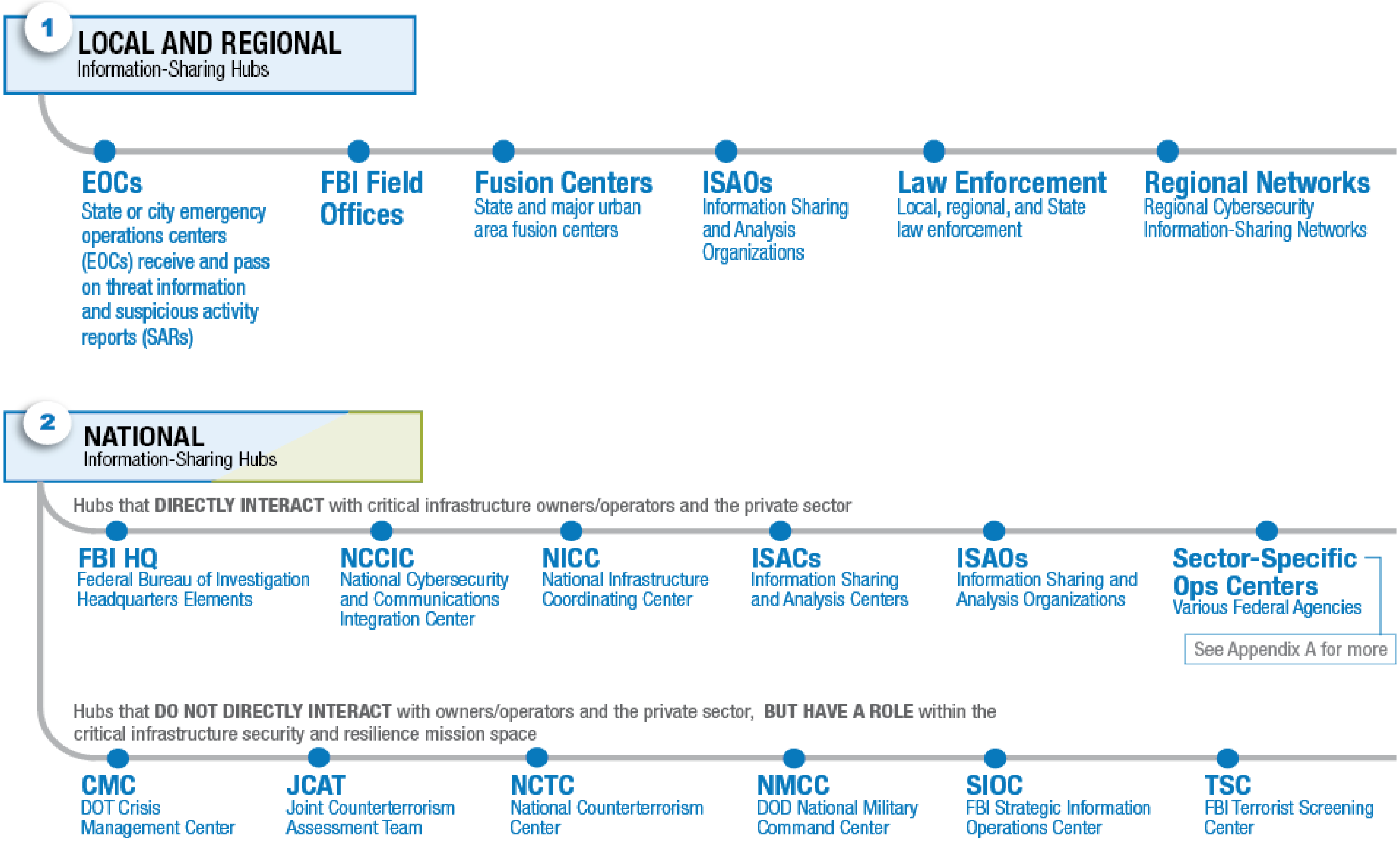
Lessons learned and case studies to improve relevance, usefulness, and format.

↕ THREAT INFORMATION

↕ ALTERNATE PATH

Key Threat Information Sharing Entities





1 **LOCAL AND REGIONAL**
Information-Sharing Hubs

EOCs
State or city emergency operations centers (EOCs) receive and pass on threat information and suspicious activity reports (SARs)

FBI Field Offices

Fusion Centers
State and major urban area fusion centers

ISAOs
Information Sharing and Analysis Organizations

Law Enforcement
Local, regional, and State law enforcement

Regional Networks
Regional Cybersecurity Information-Sharing Networks

2 **NATIONAL**
Information-Sharing Hubs

Hubs that **DIRECTLY INTERACT** with critical infrastructure owners/operators and the private sector

FBI HQ
Federal Bureau of Investigation Headquarters Elements

NCCIC
National Cybersecurity and Communications Integration Center

NICC
National Infrastructure Coordinating Center

ISACs
Information Sharing and Analysis Centers

ISAOs
Information Sharing and Analysis Organizations

Sector-Specific Ops Centers
Various Federal Agencies

See Appendix A for more

Hubs that **DO NOT DIRECTLY INTERACT** with owners/operators and the private sector, **BUT HAVE A ROLE** within the critical infrastructure security and resilience mission space

CMC
DOT Crisis Management Center

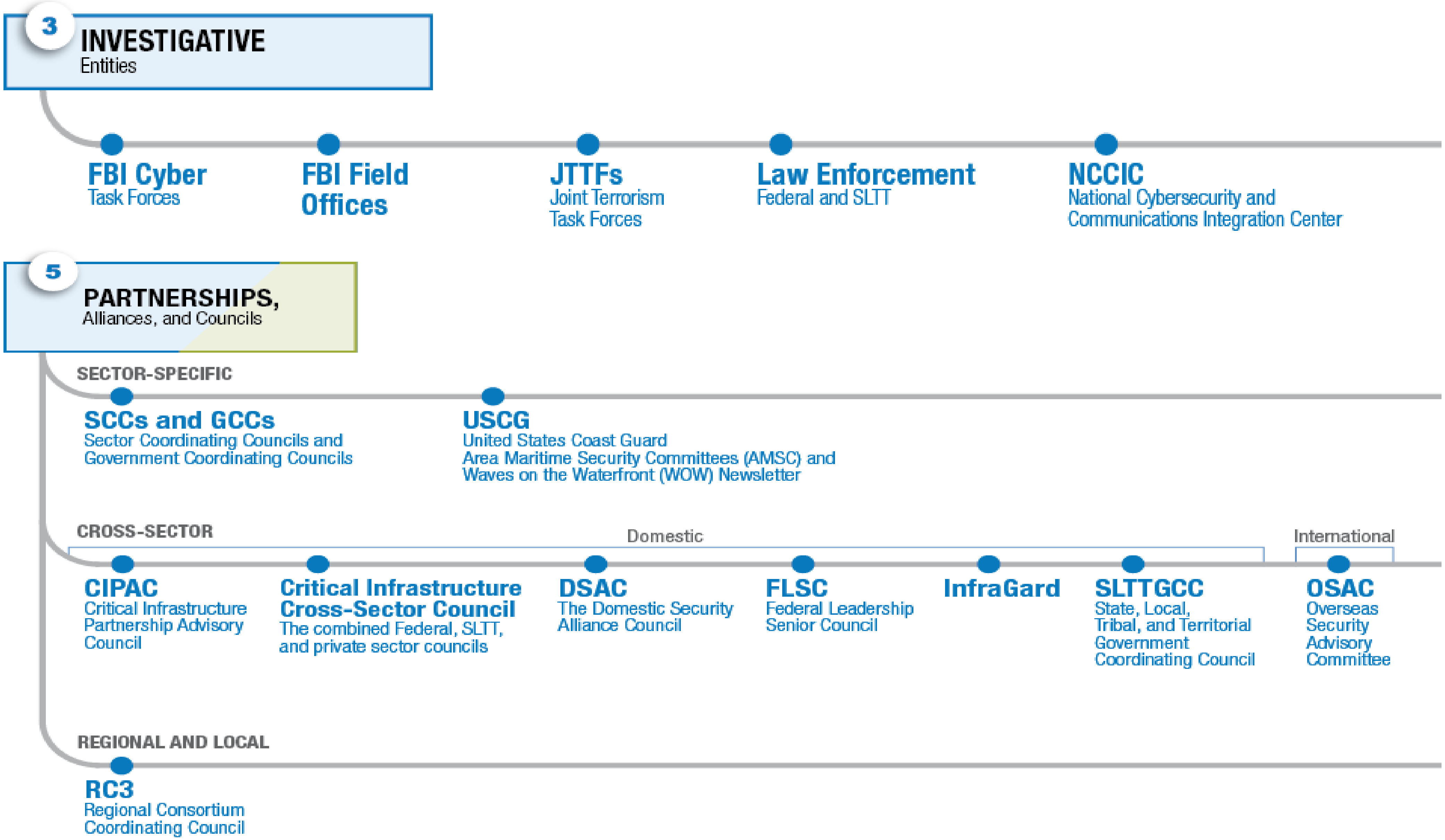
JCAT
Joint Counterterrorism Assessment Team

NCTC
National Counterterrorism Center

NMCC
DOD National Military Command Center

SIOC
FBI Strategic Information Operations Center

TSC
FBI Terrorist Screening Center



3 INVESTIGATIVE
Entities

FBI Cyber
Task Forces

FBI Field Offices

JTTFs
Joint Terrorism Task Forces

Law Enforcement
Federal and SLTT

NCCIC
National Cybersecurity and Communications Integration Center

5 PARTNERSHIPS,
Alliances, and Councils

SECTOR-SPECIFIC

SCCs and GCCs
Sector Coordinating Councils and Government Coordinating Councils

USCG
United States Coast Guard
Area Maritime Security Committees (AMSC) and Waves on the Waterfront (WOW) Newsletter

CROSS-SECTOR

Domestic

CIPAC
Critical Infrastructure Partnership Advisory Council

Critical Infrastructure Cross-Sector Council
The combined Federal, SLTT, and private sector councils

DSAC
The Domestic Security Alliance Council

FLSC
Federal Leadership Senior Council

InfraGard

SLTTGCC
State, Local, Tribal, and Territorial Government Coordinating Council

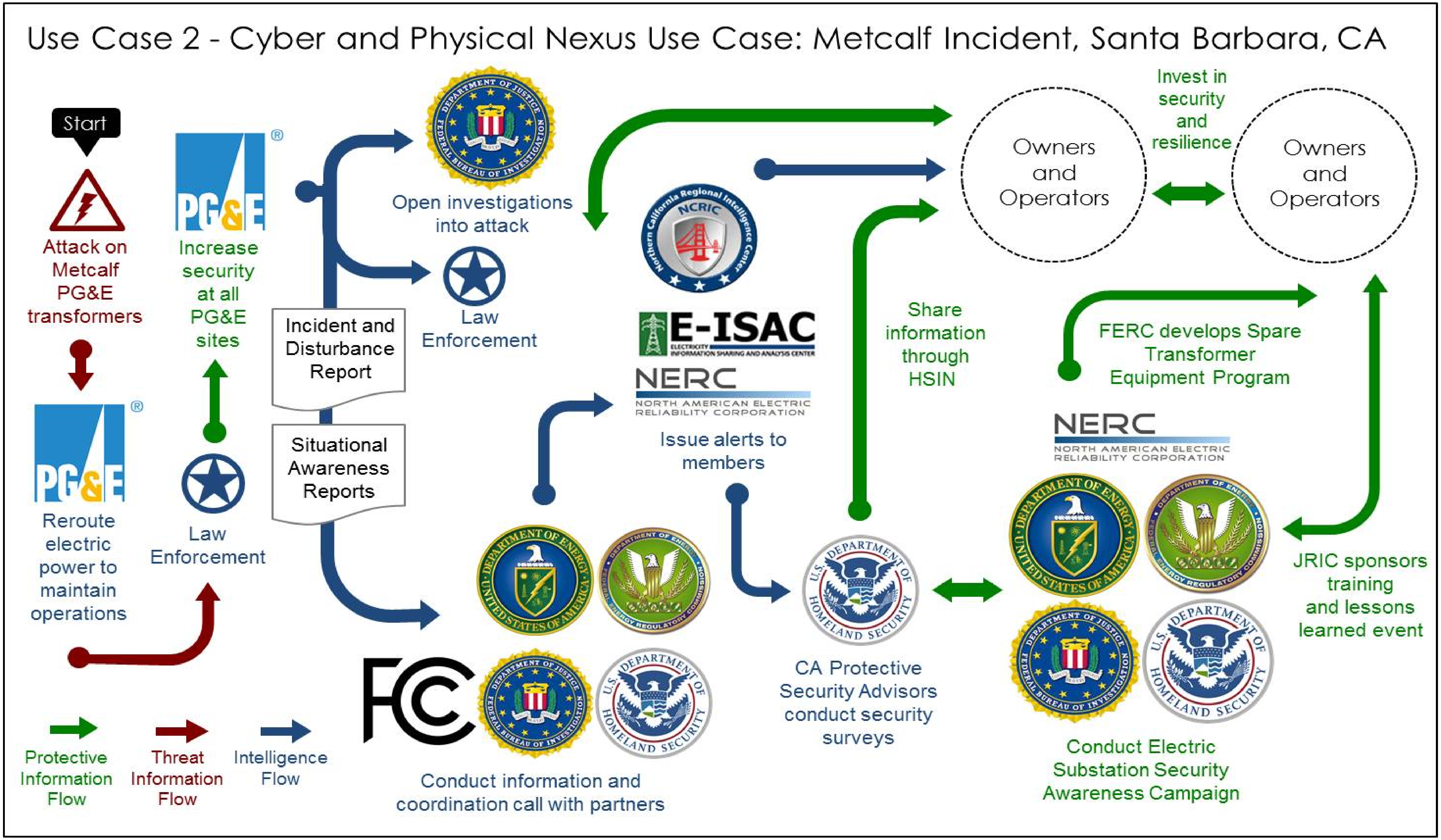
International

OSAC
Overseas Security Advisory Committee

REGIONAL AND LOCAL

RC3
Regional Consortium Coordinating Council

Case Studies



Use Case 2 - Cyber and Physical Nexus Use Case: Metcalf Incident, Santa Barbara, CA

Start

Attack on Metcalf PG&E transformers

Reroute electric power to maintain operations

Law Enforcement

Increase security at all PG&E sites

Incident and Disturbance Report

Situational Awareness Reports

Open investigations into attack

Law Enforcement

Conduct information and coordination call with partners

Issue alerts to members

CA Protective Security Advisors conduct security surveys

Share information through HSIN

Owners and Operators

Invest in security and resilience

Owners and Operators

FERC develops Spare Transformer Equipment Program

Conduct Electric Substation Security Awareness Campaign

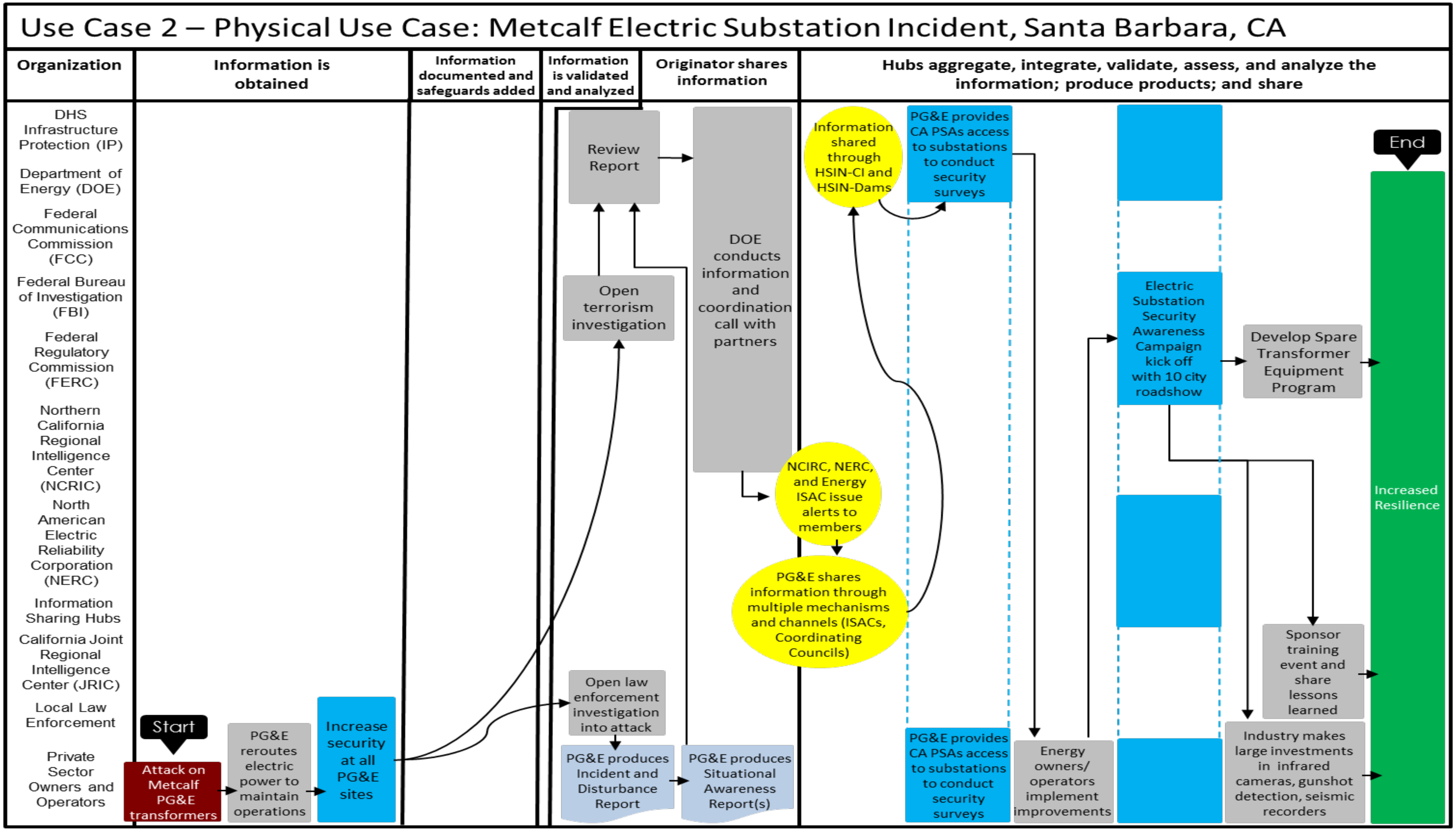
JRIC sponsors training and lessons learned event

Protective Information Flow

Threat Information Flow

Intelligence Flow

Information Flow Maps



Use Case 2 – Physical Use Case: Metcalf Electric Substation Incident, Santa Barbara, CA

Organization

Information is obtained

Information documented and safeguards added

Information is validated and analyzed

Originator shares information

Hubs aggregate, integrate, validate, assess, and analyze the information; produce products; and share

DHS Infrastructure Protection (IP)

Department of Energy (DOE)

Federal Communications Commission (FCC)

Federal Bureau of Investigation (FBI)

Federal Regulatory Commission (FERC)

Northern California Regional Intelligence Center (NCRIC)

North American Electric Reliability Corporation (NERC)

Information Sharing Hubs

California Joint Regional Intelligence Center (JRIC)

Local Law Enforcement

Private Sector Owners and Operators

Start

Attack on Metcalf PG&E transformers

PG&E reroutes electric power to maintain operations

Increase security at all PG&E sites

Review Report

Open terrorism investigation

Open law enforcement investigation into attack

PG&E produces Incident and Disturbance Report

PG&E produces Situational Awareness Report(s)

DOE conducts information and coordination call with partners

NCIRC, NERC, and Energy ISAC issue alerts to members

PG&E shares information through multiple mechanisms and channels (ISACs, Coordinating Councils)

Information shared through HSIN-CI and HSIN-Dams

PG&E provides CA PSAs access to substations to conduct security surveys

PG&E provides CA PSAs access to substations to conduct security surveys

Energy owners/ operators implement improvements

Electric Substation Security Awareness Campaign kick off with 10 city roadshow

Develop Spare Transformer Equipment Program

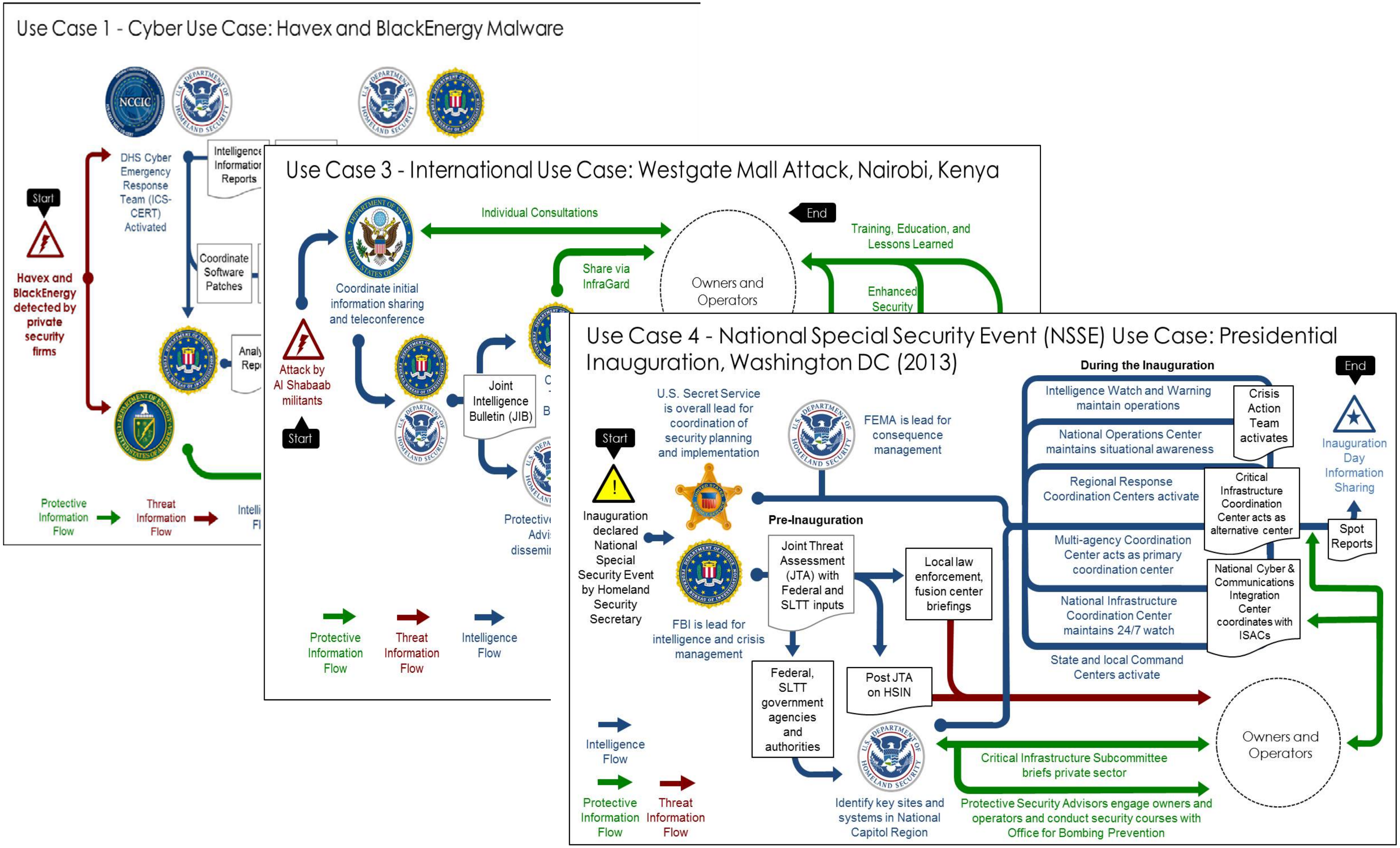
Sponsor training event and share lessons learned

Industry makes large investments in infrared cameras, gunshot detection, seismic recorders

Increased Resilience

End

Additional Case Studies



Use Case 1 - Cyber Use Case: Havex and BlackEnergy Malware

Start

Havex and BlackEnergy detected by private security firms

DHS Cyber Emergency Response Team (ICS-CERT) Activated

Intelligence Information Reports

Coordinate Software Patches

Analy Repo

Protective Information Flow

Threat Information Flow

Intelli Fl

Use Case 3 - International Use Case: Westgate Mall Attack, Nairobi, Kenya

Individual Consultations

End

Training, Education, and Lessons Learned

Share via InfraGard

Owners and Operators

Enhanced Security

Coordinate initial information sharing and teleconference

Attack by Al Shabaab militants

Start

Joint Intelligence Bulletin (JIB)

Protective Advi dissemi

Protective Information Flow

Threat Information Flow

Intelligence Flow

Use Case 4 - National Special Security Event (NSSE) Use Case: Presidential Inauguration, Washington DC (2013)

During the Inauguration

End

Intelligence Watch and Warning maintain operations

Crisis Action Team activates

National Operations Center maintains situational awareness

Inauguration Day Information Sharing

Regional Response Coordination Centers activate

Critical Infrastructure Coordination Center acts as alternative center

Multi-agency Coordination Center acts as primary coordination center

Spot Reports

National Cyber & Communications Integration Center coordinates with ISACs

National Infrastructure Coordination Center maintains 24/7 watch

State and local Command Centers activate

U.S. Secret Service is overall lead for coordination of security planning and implementation

FEMA is lead for consequence management

Start

Inauguration declared National Special Security Event by Homeland Security Secretary

Pre-Inauguration

Joint Threat Assessment (JTA) with Federal and SLTT inputs

Local law enforcement, fusion center briefings

FBI is lead for intelligence and crisis management

Federal, SLTT government agencies and authorities

Post JTA on HSIN

Owners and Operators

Critical Infrastructure Subcommittee briefs private sector

Intelligence Flow

Protective Information Flow

Threat Information Flow

Identify key sites and systems in National Capitol Region

Protective Security Advisors engage owners and operators and conduct security courses with Office for Bombing Prevention

Some Observations

Role of informal networks

Balance between too much and not enough is difficult

ISAO EO is very helpful…needs to include all hazards

Challenge of classified information

Disconnect between physical and cyber security staff

Questions?

Brian Scully

Director, Strategy and Policy Programs

DHS/NPPD/Office of Infrastructure Protection

Brian.scully1@hq.dhs.gov

Find the Framework online:

https://www.dhs.gov/publication/ci-threat-info-sharing-framework

U.S. DEPARTMENT OF HOMELAND SECURITY

Homeland
Security

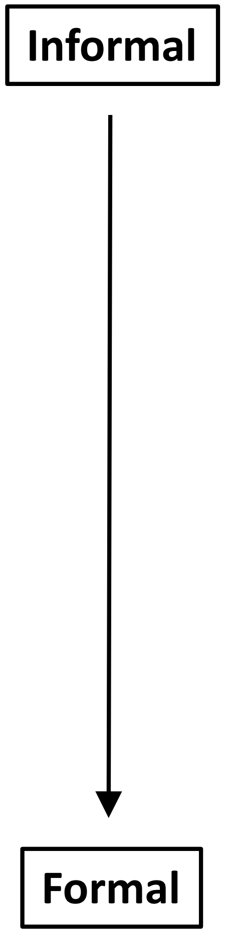
Communications Sector Information Sharing

- Information Sharing is not new to Communication Service Providers

- Information Sharing by network service providers is deep and systemic, but not fully recognized.
  - Current Efforts to Characterize and Catalogue major Venues/Opportunities for Info-Sharing
  - CSRIC V – Working Group 5 Information Sharing
    - https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability

- Primary Venue for Collaboration and Information Sharing:
  - DHS National Coordinating Center / Communications Information Sharing and Analysis Center (ISAC)
  - Public/Private Coordination Point for Physical AND Cyber Events

Info-Sharing Modalities

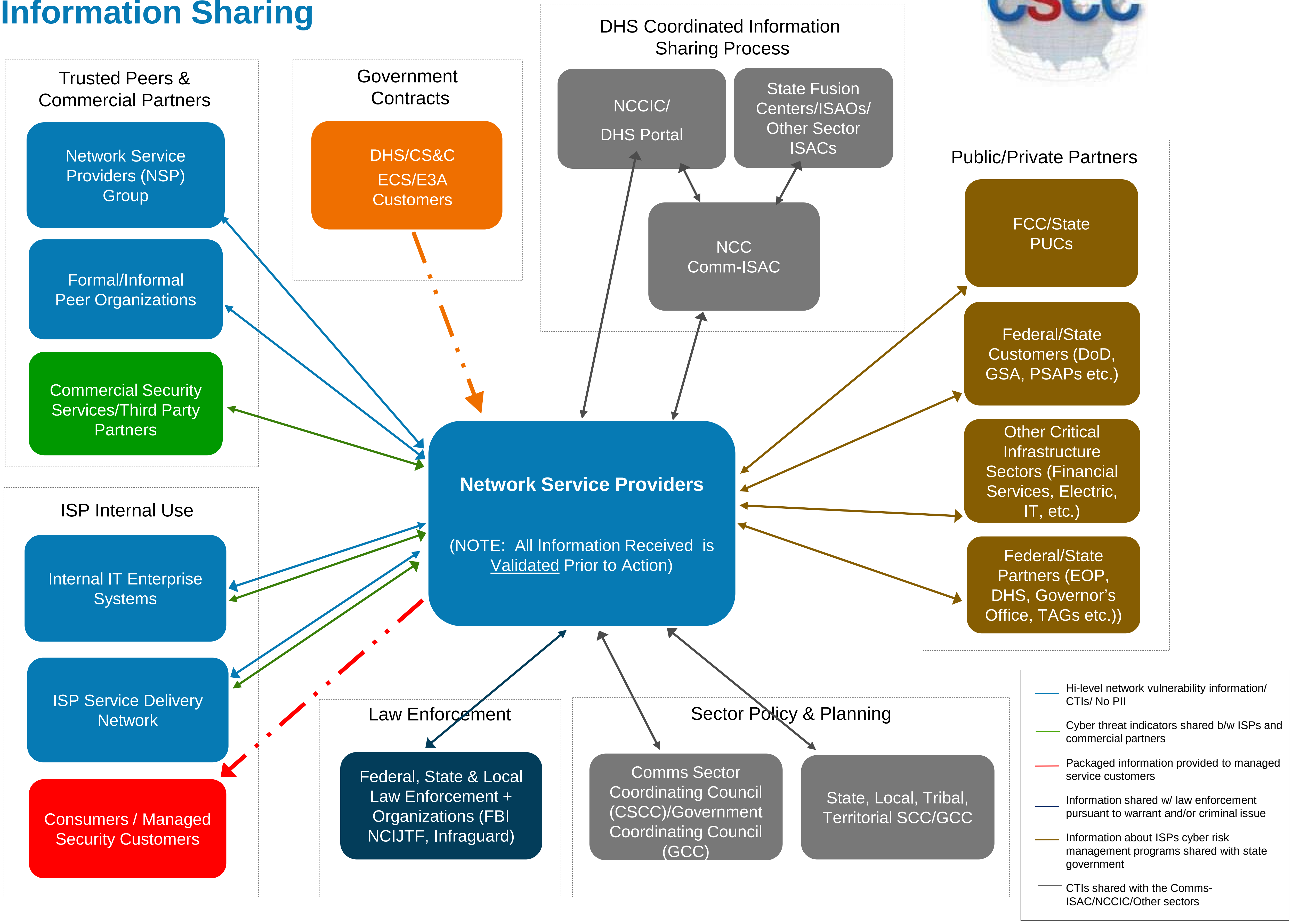


Informal

Phone Call
E-mail
Teleconference
Professional Membership
Working Group
Professional Conference
Webinar
Technical Liaison
Technical Seminar or Conference
Tabletop Exercise
Full Scale Exercise
Automated Sharing

Formal

Notional Diagram Communications Sector Information Sharing



Trusted Peers & Commercial Partners

Network Service Providers (NSP) Group

Formal/Informal Peer Organizations

Commercial Security Services/Third Party Partners

Government Contracts

DHS/CS&C ECS/E3A Customers

DHS Coordinated Information Sharing Process

NCCIC/ DHS Portal

State Fusion Centers/ISAOs/ Other Sector ISACs

NCC Comm-ISAC

Public/Private Partners

FCC/State PUCs

Federal/State Customers (DoD, GSA, PSAPs etc.)

Other Critical Infrastructure Sectors (Financial Services, Electric, IT, etc.)

Federal/State Partners (EOP, DHS, Governor's Office, TAGs etc.))

Network Service Providers

(NOTE: All Information Received is Validated Prior to Action)

ISP Internal Use

Internal IT Enterprise Systems

ISP Service Delivery Network

Consumers / Managed Security Customers

Law Enforcement

Federal, State & Local Law Enforcement + Organizations (FBI NCIJTF, Infraguard)

Sector Policy & Planning

Comms Sector Coordinating Council (CSCC)/Government Coordinating Council (GCC)

State, Local, Tribal, Territorial SCC/GCC

— Hi-level network vulnerability information/ CTIs/ No PII

— Cyber threat indicators shared b/w ISPs and commercial partners

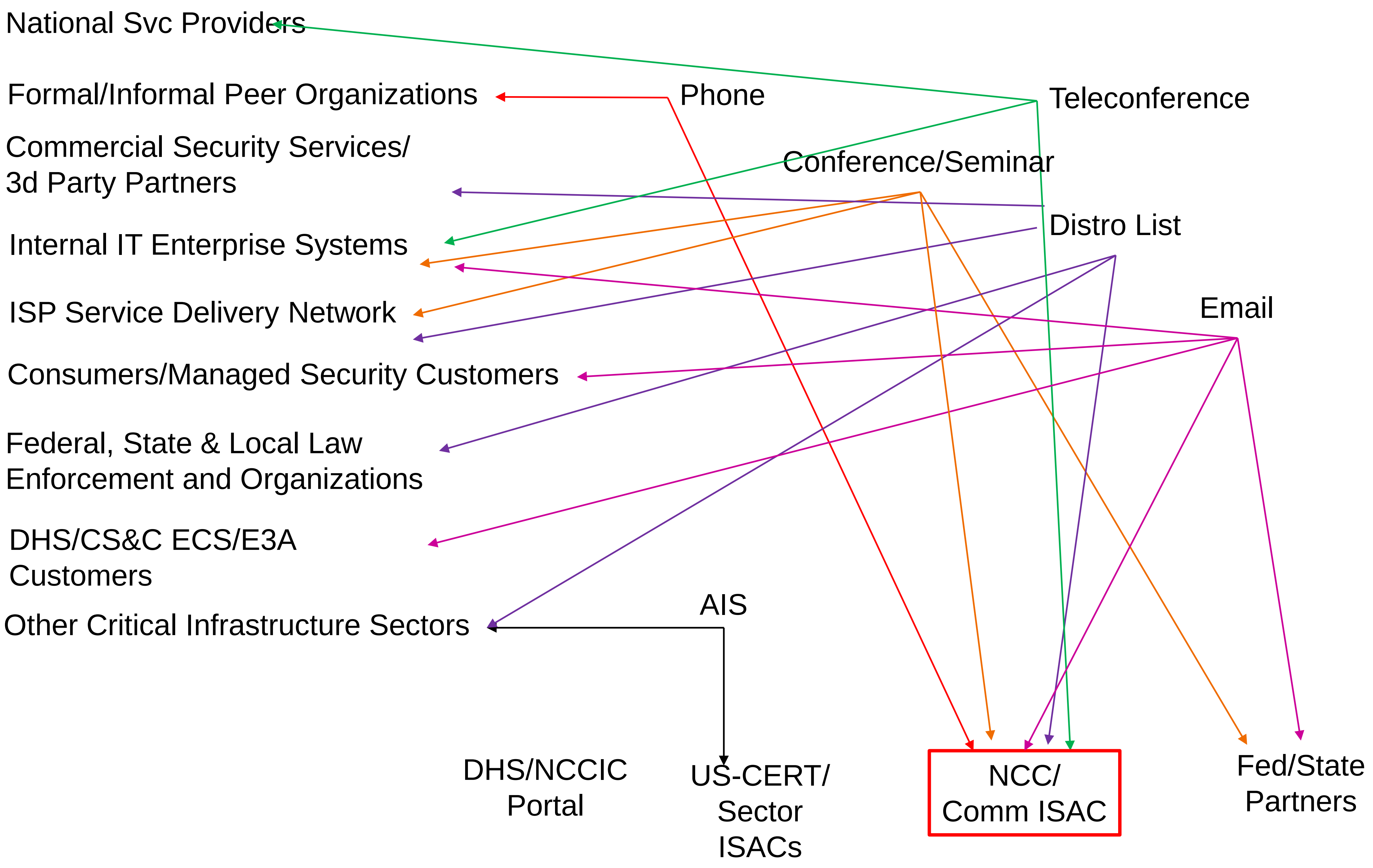
— Packaged information provided to managed service customers

— Information shared w/ law enforcement pursuant to warrant and/or criminal issue

— Information about ISPs cyber risk management programs shared with state government

— CTIs shared with the Comms-ISAC/NCCIC/Other sectors

Information Sharing Matrix



National Svc Providers

Formal/Informal Peer Organizations

Commercial Security Services/
3d Party Partners

Internal IT Enterprise Systems

ISP Service Delivery Network

Consumers/Managed Security Customers

Federal, State & Local Law
Enforcement and Organizations

DHS/CS&C ECS/E3A
Customers

Other Critical Infrastructure Sectors

Phone

Teleconference

Conference/Seminar

Distro List

Email

AIS

DHS/NCCIC
Portal

US-CERT/
Sector
ISACs

NCC/
Comm ISAC

Fed/State
Partners

Moving Forward – Continuous Improvement

- Information Sharing & Analysis Organizations (ISAOs)

- Network Service Provider Refinements

- Automated Indicator Sharing Initiatives

- International Collaboration