Northeastern University
Global Resilience Institute

“CINET: Building a Resilient Network for Critical Infrastructure”

Robert Knake
Senior Research Scientist-Cybersecurity
Global Resilience Institute
r.knake@northeastern.edu

The need: 3 interrelated problems

Critical Infrastructure owners and operators lack a secure means to communicate with each other and with the government in the event that public networks are under threat, disrupted, or cannot be trusted.

WEAK INFORMATION SHARING

Government and private sector partners cannot engage in secure communications on threats

NO NETWORK FOR RESTORATION

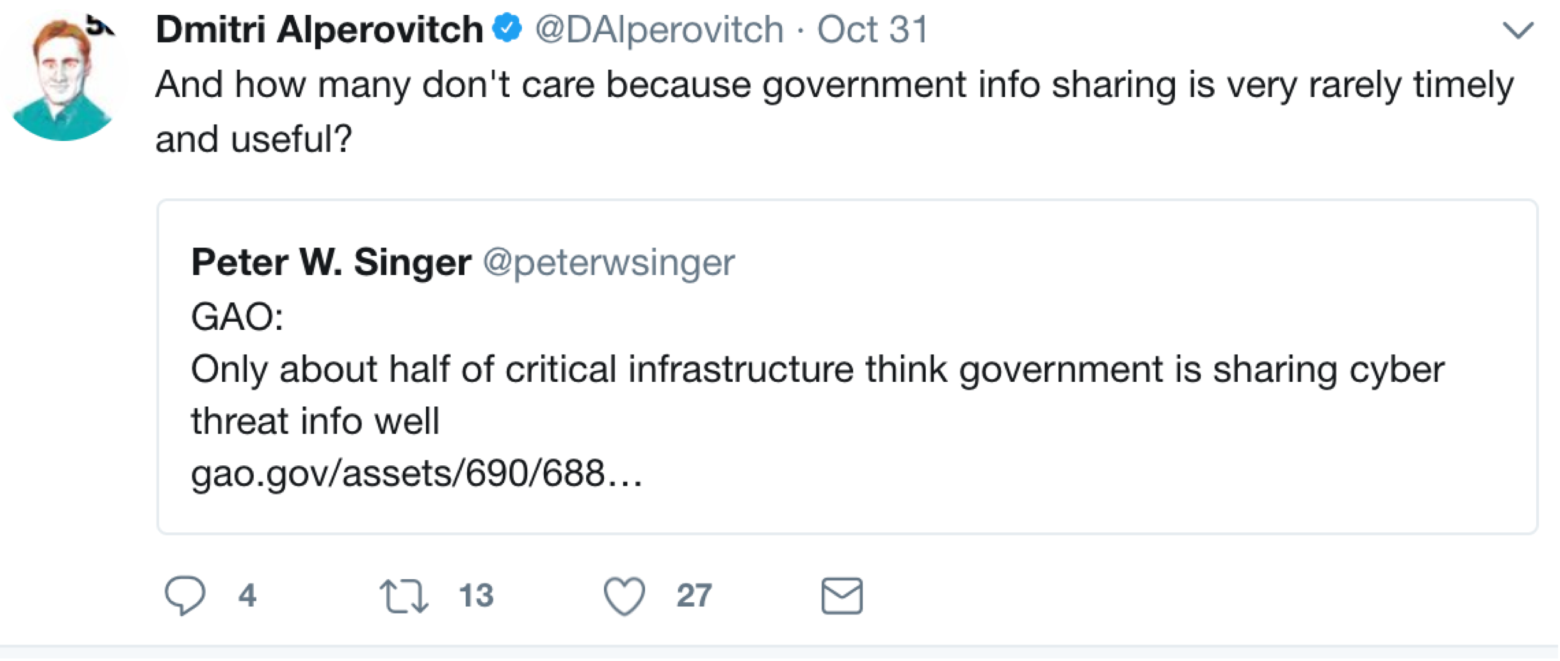
In the event of a widespread Internet outage, carriers do not have the means to coordinate restart

NON-ASSURED COMMUNICATIONS

Critical Infrastructure relies on the public internet for command and control of even the most sensitive systems

Unclassified information sharing solutions are only partial answers

- Not all information can be declassified
- Compromised networks should not be used for coordinating incident response



Dmitri Alperovitch @DAlperovitch · Oct 31

And how many don't care because government info sharing is very rarely timely and useful?

Peter W. Singer @peterwsinger

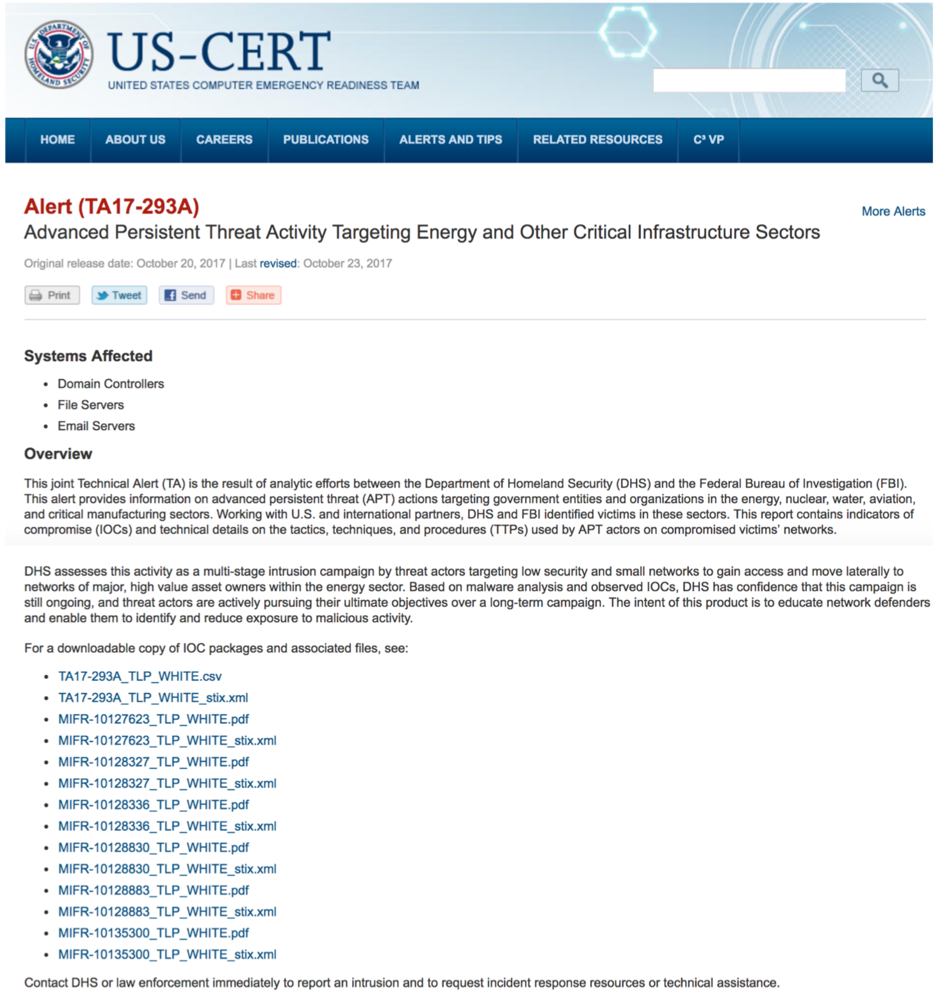
GAO:
Only about half of critical infrastructure think government is sharing cyber threat info well
gao.gov/assets/690/688…

Radio-based and other “out-of-band” communications are untested

- Government defunded federal network to provide communications mechanism for restoring the public Internet in 2013
- Old “copper wire” is being removed from network and no longer provides end-to-end communications
- Notion of using ham radio is unproven

Point solutions for cyber defense of CI have repeatedly failed

- Defending thousands of IOT devices connected by the public Internet is a hopeless task
- Limiting access is the only viable solution to provide high degrees of assurance



Alert (TA17-293A)

Advanced Persistent Threat Activity Targeting Energy and Other Critical Infrastructure Sectors

Original release date: October 20, 2017 | Last revised: October 23, 2017

Systems Affected

- Domain Controllers
- File Servers
- Email Servers

Overview

This joint Technical Alert (TA) is the result of analytic efforts between the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI). This alert provides information on advanced persistent threat (APT) actions targeting government entities and organizations in the energy, nuclear, water, aviation, and critical manufacturing sectors. Working with U.S. and international partners, DHS and FBI identified victims in these sectors. This report contains indicators of compromise (IOCs) and technical details on the tactics, techniques, and procedures (TTPs) used by APT actors on compromised victims' networks.

DHS assesses this activity as a multi-stage intrusion campaign by threat actors targeting low security and small networks to gain access and move laterally to networks of major, high value asset owners within the energy sector. Based on malware analysis and observed IOCs, DHS has confidence that this campaign is still ongoing, and threat actors are actively pursuing their ultimate objectives over a long-term campaign. The intent of this product is to educate network defenders and enable them to identify and reduce exposure to malicious activity.

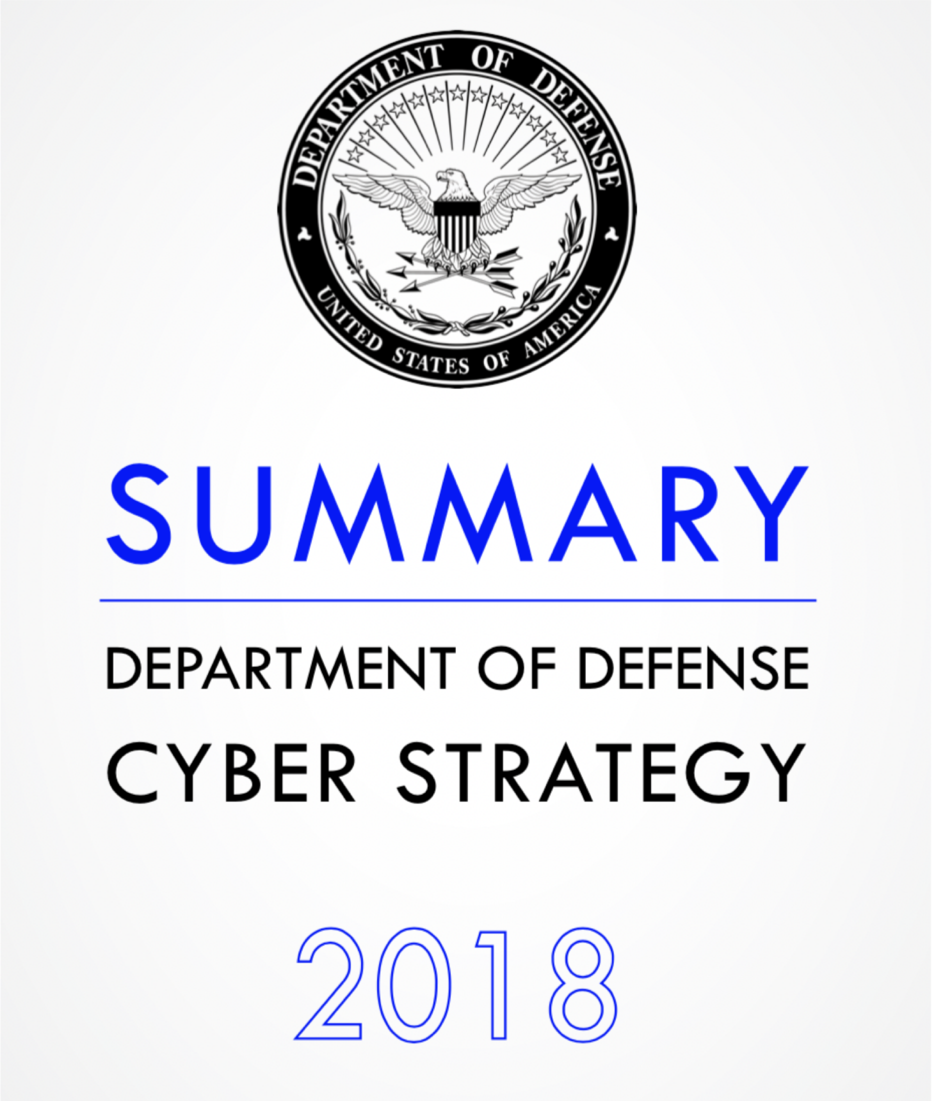
For a downloadable copy of IOC packages and associated files, see:

- TA17-293A_TLP_WHITE.csv
- TA17-293A_TLP_WHITE_stix.xml
- MIFR-10127623_TLP_WHITE.pdf
- MIFR-10127623_TLP_WHITE_stix.xml
- MIFR-10128327_TLP_WHITE.pdf
- MIFR-10128327_TLP_WHITE_stix.xml
- MIFR-10128336_TLP_WHITE.pdf
- MIFR-10128336_TLP_WHITE_stix.xml
- MIFR-10128830_TLP_WHITE.pdf
- MIFR-10128830_TLP_WHITE_stix.xml
- MIFR-10128883_TLP_WHITE.pdf
- MIFR-10128883_TLP_WHITE_stix.xml
- MIFR-10135300_TLP_WHITE.pdf
- MIFR-10135300_TLP_WHITE_stix.xml

Contact DHS or law enforcement immediately to report an intrusion and to request incident response resources or technical assistance.

Coordinating the Offense

…the Department seeks to preempt, defeat, or deter malicious cyber activity targeting U.S. critical infrastructure that could cause a significant cyber incident regardless of whether that incident would impact DoD's warfighting readiness or capability. Our primary role in this homeland defense mission is to defend forward by leveraging our focus outward to stop threats before they reach their targets. (P. 2)



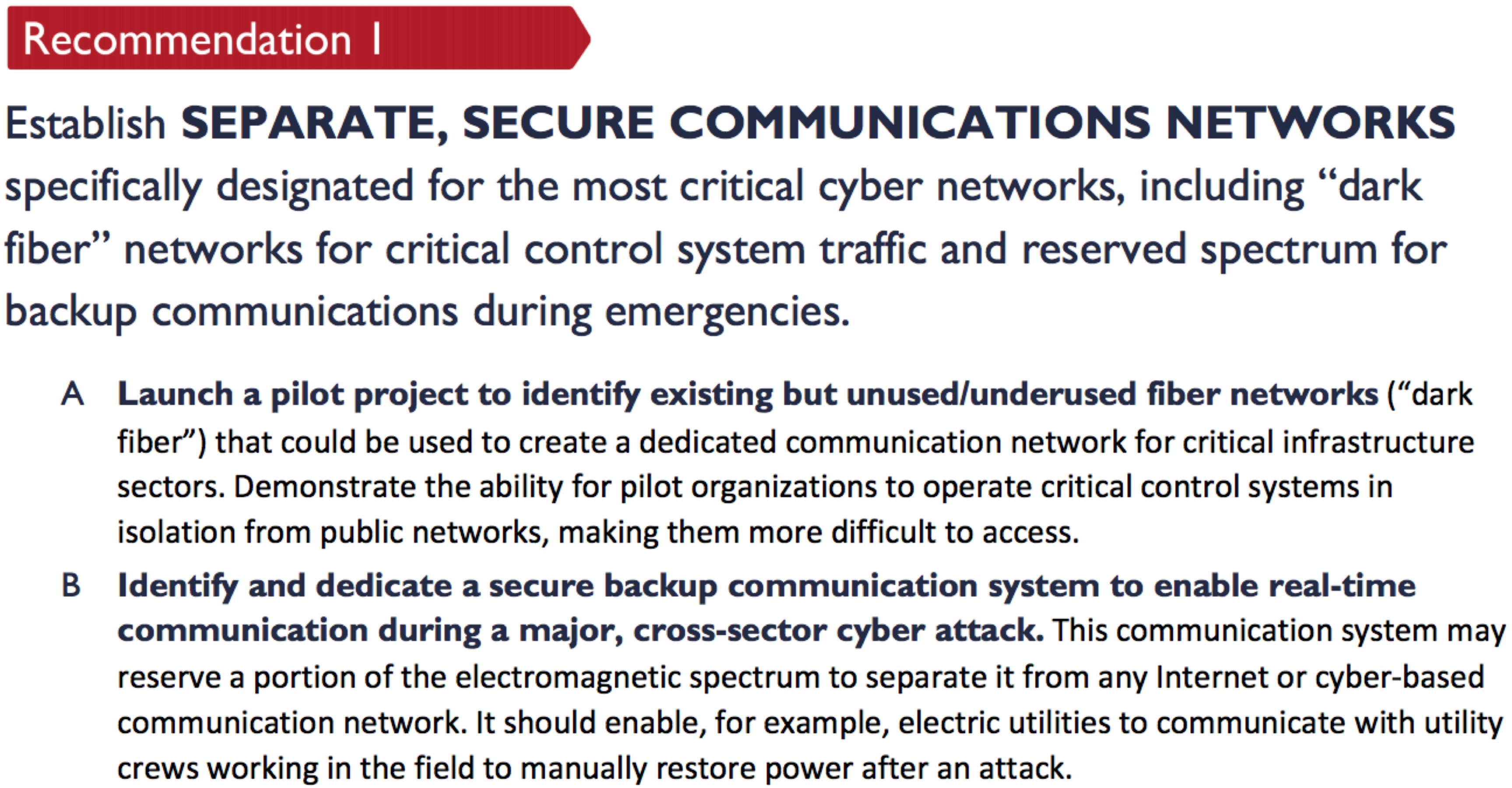
SUMMARY

DEPARTMENT OF DEFENSE

CYBER STRATEGY

2018

Proposed Solution:
CRITICAL INFRASTRUCTURE NETWORK (CINET)



Recommendation 1

Establish **SEPARATE, SECURE COMMUNICATIONS NETWORKS** specifically designated for the most critical cyber networks, including "dark fiber" networks for critical control system traffic and reserved spectrum for backup communications during emergencies.

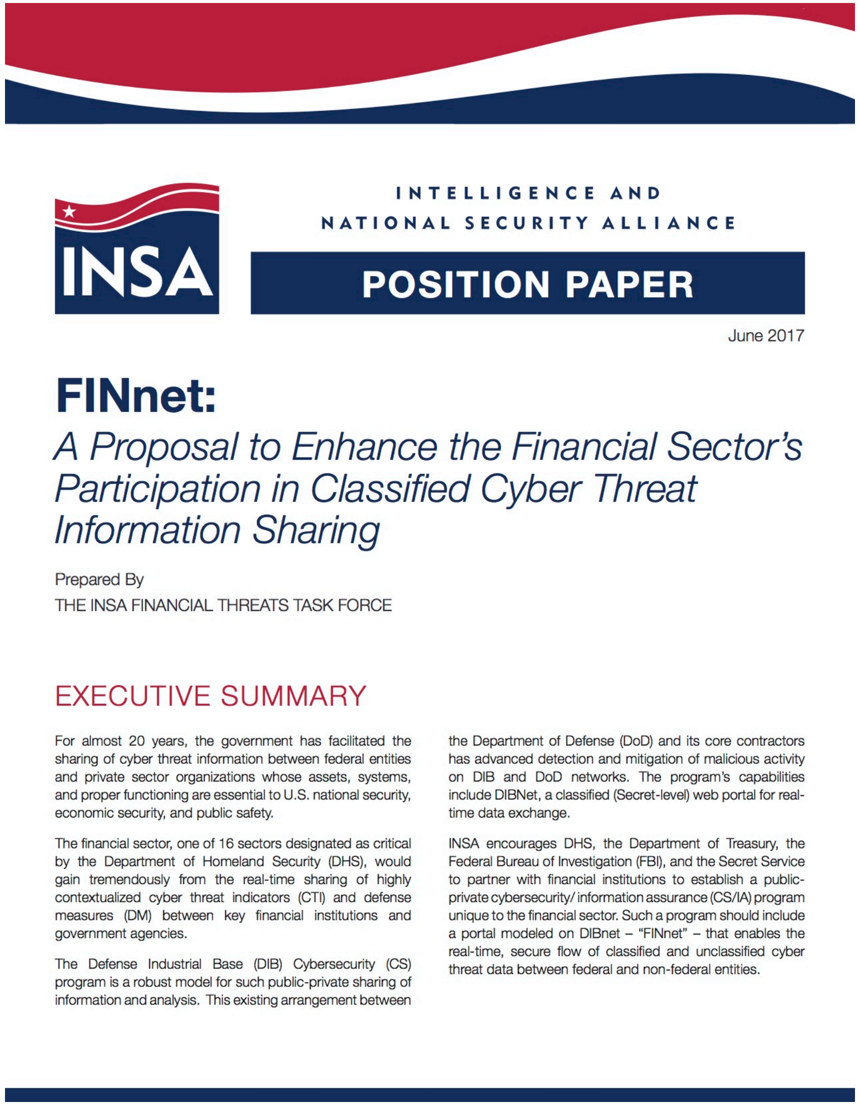
A **Launch a pilot project to identify existing but unused/underused fiber networks** ("dark fiber") that could be used to create a dedicated communication network for critical infrastructure sectors. Demonstrate the ability for pilot organizations to operate critical control systems in isolation from public networks, making them more difficult to access.

B **Identify and dedicate a secure backup communication system to enable real-time communication during a major, cross-sector cyber attack.** This communication system may reserve a portion of the electromagnetic spectrum to separate it from any Internet or cyber-based communication network. It should enable, for example, electric utilities to communicate with utility crews working in the field to manually restore power after an attack.

-- Recommendation of the National Infrastructure Advisory Council, August 2017

Build on the Success of the DIBnet Program

- The Defense Industrial Base (DIB) Cybersecurity (CS) program is a model for public-private sharing of information and analysis.
- This existing arrangement between the Department of Defense (DoD) and its core contractors has advanced detection and mitigation of malicious activity on DIB and DoD networks.
- The program's capabilities include DIBNet, a classified (Secret-level) web portal for real-time data exchange.



INSA

INTELLIGENCE AND NATIONAL SECURITY ALLIANCE

POSITION PAPER

June 2017

FINnet:

A Proposal to Enhance the Financial Sector's Participation in Classified Cyber Threat Information Sharing

Prepared By

THE INSA FINANCIAL THREATS TASK FORCE

EXECUTIVE SUMMARY

For almost 20 years, the government has facilitated the sharing of cyber threat information between federal entities and private sector organizations whose assets, systems, and proper functioning are essential to U.S. national security, economic security, and public safety.

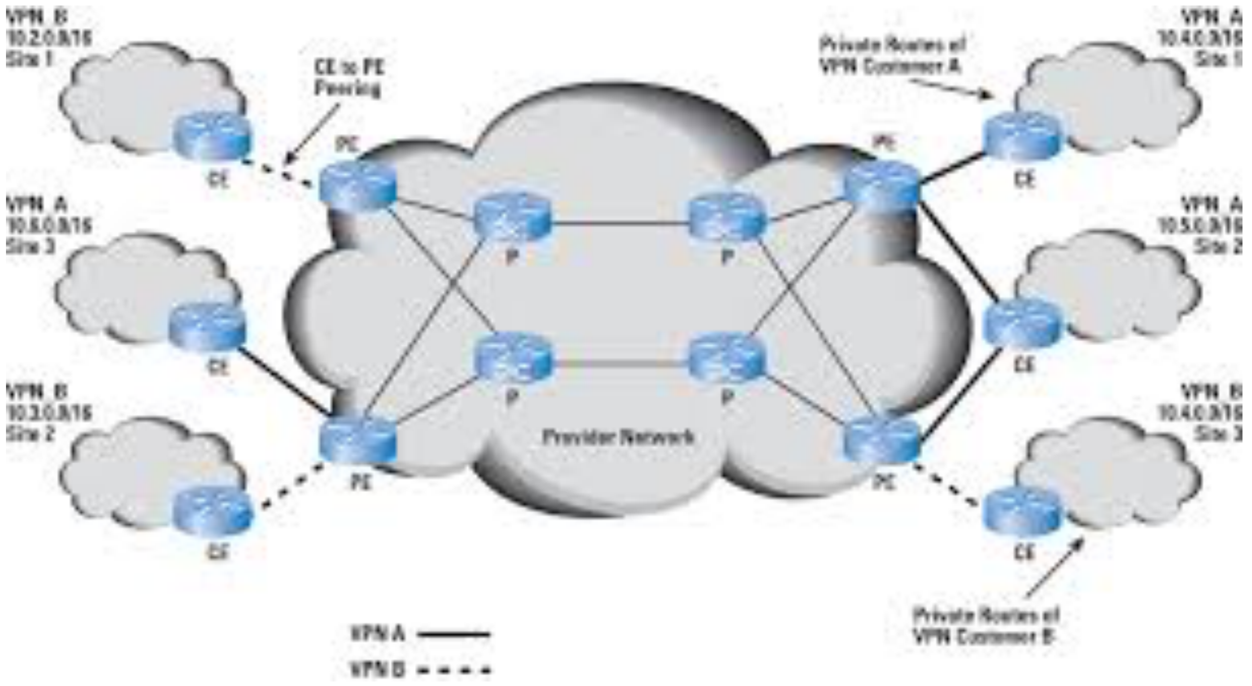
The financial sector, one of 16 sectors designated as critical by the Department of Homeland Security (DHS), would gain tremendously from the real-time sharing of highly contextualized cyber threat indicators (CTI) and defense measures (DM) between key financial institutions and government agencies.

The Defense Industrial Base (DIB) Cybersecurity (CS) program is a robust model for such public-private sharing of information and analysis. This existing arrangement between the Department of Defense (DoD) and its core contractors has advanced detection and mitigation of malicious activity on DIB and DoD networks. The program's capabilities include DIBNet, a classified (Secret-level) web portal for real-time data exchange.

INSA encourages DHS, the Department of Treasury, the Federal Bureau of Investigation (FBI), and the Secret Service to partner with financial institutions to establish a public-private cybersecurity/ information assurance (CS/IA) program unique to the financial sector. Such a program should include a portal modeled on DIBnet – "FINnet" – that enables the real-time, secure flow of classified and unclassified cyber threat data between federal and non-federal entities.

Preliminary Study: Technical Design

- Examining options for technical design of on-ramp/off ramps to move data between public Internet and CINET
- Technical challenge is movement of IoT data from public Internet to CINET
- Examining options for internal network security: immutable audit logs, built-in attribution, role-based access permissions

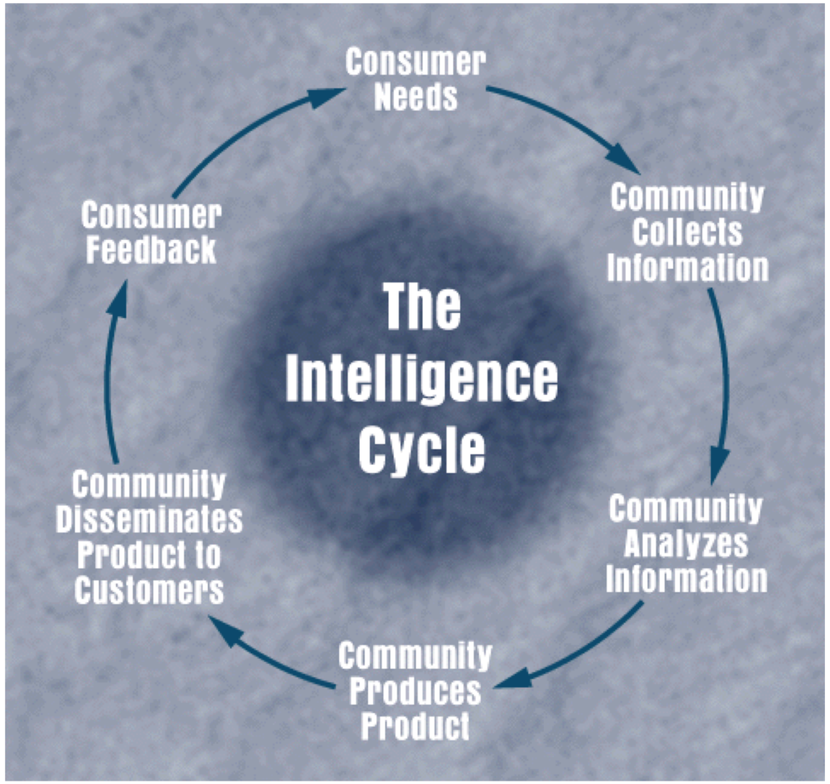


Minimally Viable Operation for Info-Sharing

- Stand up portal
- USG assigns intel analysts
- USG clears private sector personnel
- Provides facility access and notifies of new information via unclassified means
- Participants need:
  - Vault
  - Secure Phone
  - Laptop

Value Proposition for Intel Sharing

- Better information
- Two-way collaboration with government
- Secure communication and collaboration among pilot members
- Malware analysis and forensics support from government labs


The Intelligence Cycle
Consumer Needs
Community Collects Information
Community Analyzes Information
Community Produces Product
Community Disseminates Product to Customers
Consumer Feedback

Next Steps for Operational Network Concept

1. Determine technical feasibility
2. Determine security value
3. Identify funding source and mechanism

Northeastern University

Global Resilience Institute