Working Group 5:
Cybersecurity Information Sharing

Status Update

March 16, 2016

Christopher Boyer, Co-Chair (AT&T)
Rod Rasmussen, Co-Chair (Infoblox)
Brian Allen, Co-Chair (Time Warner Cable)

WG5 Description

- In order to improve the communication sector's ability to identify, protect, detect, respond, and recover from cyber attacks, Working Group 5 will develop recommendations to the Council encourage sharing of cybersecurity information between companies in the communications sector.

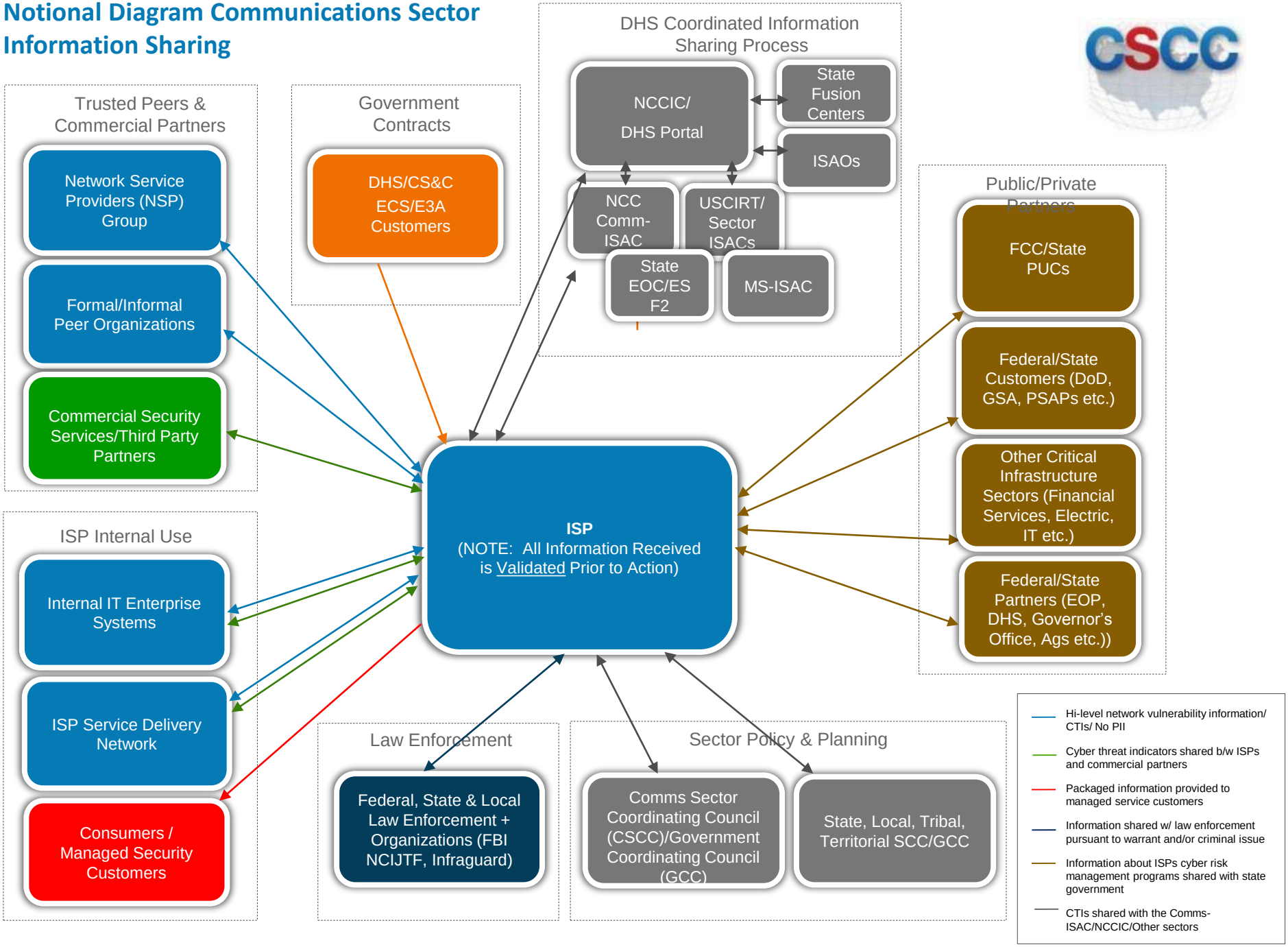
WG5 Members

Name	Company	Name (cont.)	Company (cont.)
Chris Boyer (Co-Chair)	AT&T	Robert Gessner	MCTV
Rod Rasmussen (Co-Chair)	Infoblox	Mark Hoffer	MCTV
Brian Allen (Co-Chair)	Time Warner Cable	Michael Robinson	MCTV
Greg Intoccia (FCC Liaison)	FCC	Bill Mertka	Motorola (ATIS)
Vern Mosley (FCC Liaison)	FCC	Larry Walke	NAB
Martin Dolly	AT&T (ATIS)	Loretta Polk	NCTA
Rosemary Leffler	AT&T	Matt Tooley	NCTA
Trace Hollifield	Bright House Networks	Dr. Donald H. Sebastian	NJ Institute of Tech
Kathryn Condello	CenturyLink	Frank Menzer	NOAA
Paul Diamond	CenturyLink	Kathy Whitbeck	Nsight
Mary Haynes	Charter	Jesse Ward	NTCA
John Kelly	Comcast Cable	Kazu Gomi	NTT America
Jorge Nieves	Comcast Cable	Shinichi Yokohama	NTT America
Paul Fournier	Comcast Cable	Michael Brown	RSA
Rudy Brioche	Comcast Cable	Richard Perlotto II	Shadowserver
Kevin Kastor	Consolidated	Jason Jenkins	SilverStar
Jemin Thakkar	Cox Communications	Jeff England	SilverStar
Matt Carothers	Cox Communications	Allison Growney	Sprint
John Marinho	CTIA	Brian Scarpelli	TIA
Chris Alexander	DHS	Joe Viens	Time Warner
John O'Connor	DHS	Chris R. Roosenraad	Time Warner Cable
Alexander Gerdenitsch	Echostar	Arthur “Trey” Jackson	T-Mobile
Jennifer Manner	Echostar	Cindy Carson	T-Mobile
David Colberg	EMC	Harold Salters	T-Mobile
Daniel Cashman	FairPoint Communications	Howard Brown	Tulalip Data Services
Carlos Carrillo	FireEye	Robert Mayer	US Telecom
Thomas M. MacLellan	FireEye	Eric Osterweil	Verisign
Tony Cole	FireEye	Shawn Wilson	Verisign
Dave Keech	Frontier	Nneka Chiazor	Verizon
Ethan Lucarelli	Iridium (Wiley Rein)	Dorothy A. Spears-Dean	VITA
Michael O'Reirdan	MAAWG	Greg Lucak	Windstream
		Kelly Fuller	WOW, Inc.

WG5 Deliverables & Timeline

- ✓ Dec 2015 - Cybersecurity Information Sharing Diagram
- ✓ Mar 2016 - Use Cases
- Jun 2016 - Impediments/Barriers and Solutions to Cybersecurity Information Sharing
- Sep 2016 - Cybersecurity Information Sharing “Trust Pools”
- Dec 2016 - Cybersecurity Information Sharing Platforms
- Mar 2017 - Recommendations for Cybersecurity Information Sharing

Notional Diagram Communications Sector Information Sharing



Sub-Group #1: Private to Private Sharing

Categorization Model

Formality of Relationship

- Formal
  - Contractual
  - Vetting In
- Informal
  - Personal relationships
  - “Open Source”

Structure of Data

- Structured
  - Data Feeds
  - Anti-Spam/Anti-Virus
  - Machine readable
- Unstructured
  - Mailing lists & Phone calls
  - Conferences
    - Formal presentations
    - “Hallway track”
  - Aimed at humans

Sub-Group #1: Private to Private Sharing

Quadrant Examples

Formal

Relationships

Informal

Formal Unstructured

- Example Organizations
  - NSP-SEC – (Network Service Provider - Security)
  - OPS-Trust (Operations Security - Trust)
  - M^{3}AAWG (Messaging, Malware and Mobile Anti-Abuse Working Group)
  - MSRA (Microsoft Security Response Alliance… formerly Global Infrastructure alliance for Internet Safety)
  - Oasis
  - Other Sector ISACs
- Security Vendor annual reports
- Data from various law enforcement

Formal Structured

- Commercial products
  - Anti-Spam
  - Anti-Phishing
  - Threat Intelligence
  - Brand Protection
- Customer Information Flows – (from Managed Services)

Informal Unstructured

- Personal Relationship (s)
- Example Organizations:
  - Infragard
  - NANOG
- Example Reports
  - Verizon Breach Report
  - SpamHaus ROKSO

Informal Structured

- Open-Source
  - Anti-Spam
  - Anti-Phishing
  - Threat Intelligence

Unstructured → Structured

Data

Sub-Group #1: Private to Private Sharing

Sample Use Case – Formal Structured

ISP & Entity Relationship	Formal, structured, information sharing between two entities with a defined relationship, such as a legal agreement. ~~This may be a commercial or~~ non-commercial agreement.
Relationship Type	Formal - structured
Information that is Shared	*To whom:* Typically this involves sharing from an entity to an ISP, e.g. from a vendor to a customer, but other arrangements may exist as well. For instance, the ISP may share data rather than money.
	Content & Value: Content is machine-readable IOCs. The format may be as simple as CSV files delivered over HTTPS, or it may be as complex as STIX delivered over TAXII.
	Timeliness: This may be anything from real time in the case of automated detection systems or sinkholes to weeks delayed in the case of manual investigation.
	Sharing Process: The process varies depending on the source of the data and the technology they have chosen.
Benefits of Information Sharing	• Compromises prevented or at least identified. • Vulnerabilities revealed, potentially prior to exploitation. • Can be used for victim notification in the case where a vendor sends an ISP lists of compromised customer IPs.
Gaps in Information & Process	• Every vendor has a different format for their data and a different method of delivery. • Every source requires custom integration. • Quality of data varies, and there is no standard to assess that quality.
Barriers & Challenges	• Vendors are often prohibitively expensive. • Integration is costly and time consuming. • Contextual data is often missing. E.g. an IP is listed as bad, but there's no further information as to why it is bad or how an ISP can determine whether a detection is a false positive.

Sub-Group #2: Private-Government-Private Use Cases

- EAS Service Disruption
- Data Breach Investigative Report
- Foreign Government to U.S. Industry
- TDOS Government and Industry Use Case
- Heartbleed
- NCFTA Government and Industry Use Case
- Government to Industry Solar Flares
- Hacktavist Threats to Law Enforcement and Public Officials
- Qakbot Botnet
- Social Engineering

Sub-Group #2: Private-Government-Private

Sample Use Case – EAS Service Disruption

Description	Poor password security allowed hackers to broadcast a bogus warning on TV networks. The FCC published an urgent advisory to change passwords on all manufacturers' equipment that forces emergency broadcasts on television networks, interrupting regular programming and to ensure the gear was secured behind firewalls. They should also inspect systems to ensure hackers had not queued "unauthorized alerts" for future transmission.
ISP & Entity Relationship	Industry to Government
Relationship Type	Formal - structured
Information that is Shared	*To whom:* Communications ISAC members and Government
	Content & Value: Emergency Alert System for three MI television stations breached, sending audio messages of zombie citing and avoidance alerts (hacking)
	Timeliness: Contacted Michigan Association of Broadcasters, State Police and FCC same day
	Sharing Process: Email notification from TV stations to MAB, police and FCC as well as NCCIC/NCC
Benefits of Information Sharing	Research, identification and mitigation of the problem at affected stations and notification of other stations to mitigate possibility of the problem being repeated
Gaps in Information & Process	None
Barriers & Challenges	Contacting all stations nationwide to reset passwords from the factory standard; message could have involved a different code causing public concern and/or panic

Next Steps

- Review barriers and challenges identified by working group.
- Schedule another face-to-face meeting in 2Q2016 timeframe.
- Draft June 2016 Interim Report to reflect barriers/challenges.
- Provide periodic status updates to Steering Committee and Council.