



Who do you think you are?

Stuart Murdoch, FIRST 2022



WHO

DO YOU THINK YOU ARE?TM





Britsoft: An Oral History

£30.00



Edited by Alex Wiltshire | Designed by Julia



Dimensions
236 × 166 mm

Binding
Hardcover

Pages
420pp

Britsoft: An Oral History is a collective story of the early British games industry. Composed of interviews with thirty-five people who shaped the modern videogame, including David Braben (*Elite*), Peter Molyneux (*Populous*), Rob Hubbard (*Commando*) and Jeff Minter (*Attack of the Mutant Camels*), it documents a vibrant period of invention in Britain's cultural history – the start of a new form of entertainment, created on ZX Spectrums, Commodore 64s, Amigas and Atari STs, in bedrooms and living rooms.





Who do you think you are?

Part one - Standards



MITRE Att&ck®

layout: side show sub-techniques hide sub-techniques

Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 42 techniques	Credential Access 16 techniques	Discovery 30 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (2)	Acquire Infrastructure (4)	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (3)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Adversary-in-the-Middle (2)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (2)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (2)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Compromise Infrastructure (6)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (14)	Boot or Logon Autostart Execution (14)	Boot or Logon Autostart Execution (14)	Credentials from Password Stores (3)	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture	Data Encoding (2)	Exfiltration Over Alternative Protocol (2)	Data Encrypted for Impact
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Obfuscation (2)	Defacement (2)	(Data Manipulation) (3)
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (2)	Inter-Process Communication (3)	Browser Extensions	Compromise Client Software Binary	Compromise Client Software Binary	Exploitation for Forced Authentication	Cloud Service Dashboard	Remote Services (4)	Clipboard Data	Dynamic Resolution (3)	Exfiltration Over C2 Channel	Disk Wipe (2)
Phishing for Information (2)	Obtain Capabilities (2)	Replication Through Removable Media	Native API	Compromise System Process (4)	Create or Modify System Process (4)	Create or Modify System Process (4)	Forge Web Credentials (2)	Cloud Storage Object Discovery	Replication Through Removable Media	Encrypted Channels	Encrypted Channel (2)	Exfiltration Over Other Network Medium (1)	Endpoint Denial of Service (4)
Search Closed Sources (2)	Stage Capabilities (3)	Supply Chain Compromise (3)	Scheduled Task/Job (5)	Domain Policy Modification (2)	Direct Volume Access	Direct Volume Access	Input Capture (4)	Container and Resource Discovery	Software Deployment Tools	Fallback Channels	Ingress Tool Transfer	Exfiltration Over Web Service (2)	Firmware Corruption
Search Open Technical Databases (4)	Trusted Relationship	Trusted Relationship	Shared Modules	Event Triggered Execution (15)	Escape to Host	Escape to Host	Modify Authentication Process (3)	Debugger Evasion	Taint Shared Content	Data from Configuration Repository (2)	Multi-Stage Channels	Exfiltration Over Medium (1)	Inhibit System Recovery
Search Open Websites/Domains (2)	Valid Accounts (4)	Valid Accounts (4)	Software Deployment Tools	External Remote Services	Event Triggered Execution (15)	Event Triggered Execution (15)	Multi-Factor Authentication Request Interception	Domain Trust Discovery	Use Alternate Authentication Material (4)	Data from Information Repositories (2)	Non-Application Layer Protocol	Exfiltration Over Web Service (2)	Network Denial of Service (2)
Search Victim-Owned Websites	Windows Management Instrumentation	Windows Management Instrumentation	System Services (2)	Hijack Execution Flow (12)	Exploitation for Privilege Escalation	Exploitation for Privilege Escalation	Network Sniffing	File and Directory Permissions Modification (2)	Group Policy Discovery	Data from Local System	Non-Standard Port	Scheduled Transfer	Resource Hijacking
			User Execution (2)	Implant Internal Image	Hijack Execution Flow (12)	Hijack Execution Flow (12)	OS Credential Dumping (4)	Network Service Discovery	Network Share Discovery	Data from Network Shared Drive	Protocol Tunneling	Transfer Data to Cloud Account	Service Stop
			Windows Management Instrumentation	Modify Authentication Process (3)	Indicator Removal on Host (3)	Indicator Removal on Host (3)	Steal Application Access Token	Network Sniffing	Password Policy Discovery	Data from Removable Media	Proxy (4)	System Shutdown/Reboot	System Shutdown/Reboot
			Office Application Startup (6)	Indirect Command Execution	Masquerading (7)	Masquerading (7)	Steal Kerberos Tickets (4)	Peripheral Device Discovery	Perimeter Device Discovery (2)	Data Staged (2)	Remote Access Software		
			Pre-OS Boot (3)	Masquerading (7)	Modify Authentication Process (3)	Modify Authentication Process (3)	Steal Web Session Cookie	Process Discovery	Permission Groups Discovery (2)	Email Collection (3)	Traffic Signaling (1)		
			Scheduled Task/Job (3)	Modify Cloud Compute Infrastructure (4)	Modify Registry	Modify Registry	Unsecured Credentials (7)	Query Registry	Process Discovery	Input Capture (4)	Web Service (3)		
			Server Software Component (3)	Modify System Image (2)	Network Boundary Bridging (1)	Network Boundary Bridging (1)		Remote System Discovery	Process Discovery	Screen Capture			
			Traffic Signaling (1)	Obfuscated Files or Information (5)	Plist File Modification	Plist File Modification		Software Discovery (1)	Query Registry	Video Capture			
			Valid Accounts (4)	Pre-OS Boot (3)	Process Injection (12)	Process Injection (12)		System Information Discovery	Remote System Discovery				
				Process Injection (12)	Reflective Code Loading	Reflective Code Loading		System Information Discovery	System Information Discovery				
				Rogue Domain Controller	Rogue Domain Controller	Rogue Domain Controller		System Location Discovery (1)	System Location Discovery (1)				
				Rootkit	Rootkit	Rootkit		System Network Configuration Discovery (1)	System Network Configuration Discovery (1)				
				Subvert Trust Controls (4)	Subvert Trust Controls (4)	Subvert Trust Controls (4)		System Network Connections Discovery	System Network Connections Discovery				
				System Binary Proxy Execution (13)	System Binary Proxy Execution (13)	System Binary Proxy Execution (13)		System Owner/User Discovery	System Owner/User Discovery				
				System Script Proxy Execution (1)	System Script Proxy Execution (1)	System Script Proxy Execution (1)		System Service Discovery	System Service Discovery				
				Template Injection	Template Injection	Template Injection		System Time Discovery	System Time Discovery				
				Traffic Signaling (1)	Traffic Signaling (1)	Traffic Signaling (1)		System Time Discovery	System Time Discovery				
				Trusted Developer Utilities Proxy Execution (1)	Trusted Developer Utilities Proxy Execution (1)	Trusted Developer Utilities Proxy Execution (1)		Virtualization/Sandbox Evasion (2)	Virtualization/Sandbox Evasion (2)				
				Unused/Unsupported Cloud Regions	Unused/Unsupported Cloud Regions	Unused/Unsupported Cloud Regions		Use Alternate Authentication Material (4)	Use Alternate Authentication Material (4)				
				Use Alternate Authentication Material (4)	Use Alternate Authentication Material (4)	Use Alternate Authentication Material (4)		Valid Accounts (4)	Valid Accounts (4)				
				Valid Accounts (4)	Valid Accounts (4)	Valid Accounts (4)		Virtualization/Sandbox Evasion (2)	Virtualization/Sandbox Evasion (2)				
				Virtualization/Sandbox Evasion (2)	Virtualization/Sandbox Evasion (2)	Virtualization/Sandbox Evasion (2)		Weaken Encryption (2)	Weaken Encryption (2)				
				Weaken Encryption (2)	Weaken Encryption (2)	Weaken Encryption (2)		XSL Script Processing	XSL Script Processing				
				XSL Script Processing	XSL Script Processing	XSL Script Processing							

Submit a CVE Request


* Required

* **Select a request type**

- Please choose an action -

* **Enter your e-mail address**

Please enter a valid e-mail address where we can reach you.

 **IMPORTANT:** Please add cve-request@mitre.org and cve@mitre.org as safe senders in your email client before completing this form.

Enter a PGP Key (to encrypt)

If you would like us to send an encrypted response, please provide a PGP key up to 20,000 characters. If your PGP key is longer than 20,000 characters, please provide a URL or contact us at cve@mitre.org to identify an alternative solution.



[[Search](#)] [[txt](#)] [[html](#)] [[pdf](#)] [[with errata](#)] [[bibtex](#)] [[Tracker](#)] [[WG](#)] [[Email](#)] [[Diff1](#)]
From: [draft-moriarty-post-inch-rid-12](#) Informational
Obsoleted by: [6545](#) [Errata exist](#)

Internet Engineering Task Force (IETF)
Request for Comments: 6045
Category: Informational
ISSN: 2070-1721

K. Moriarty
EMC
November 2010

Real-time Inter-network Defense (RID)

Abstract

Network security incidents, such as system compromises, viruses, phishing incidents, and denial of service, typically result in the loss of service, data, and resources both human and machine. Network providers and Computer Security Incident Response Teams (CSIRTs) need to be equipped and ready to assist in communicating and handling security incidents with tools and procedures in place at the time of occurrence of an attack. Real-time Inter-network Defense (RID) outlines a proactive inter-network communication method for sharing incident handling data while integrating existing tools for tracing, source identification, and mitigation mechanisms into a complete incident handling solution. Combining these tools with a communication system provides a way to achieve higher security levels on networks. Policy guidelines for handling incidents are recommended and can be agreed upon by a consortium using the security recommendations and considerations.

RID has found use within the international research communities, but has not been widely adopted in other sectors. This publication provides the specification to those communities that have adopted it, and communities currently considering solutions for real-time inter-network defense. The specification may also accelerate development of solutions where different transports or message formats are required by leveraging the data elements and structures specified here.



[[Search](#)] [[txt](#)] [[html](#)] [[pdf](#)] [[bibtex](#)] [[Tracker](#)] [[WG](#)] [[Email](#)] [[Diff1](#)] [[Diff2](#)] [[Nits](#)]

From: [draft-ietf-inch-iodef-14](#)

Proposed Standard

Obsoleted by: [7970](#)

[Errata exist](#)

Updated by: [6685](#)

Network Working Group

R. Danyliw

Number of Comments: 5070

CERT

Internet-Draft
Standards Track

J. Meijer

UNINETT

Y. Demchenko

University of Amsterdam

December 2007



The Incident Object Description Exchange Format

Status of This Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Abstract

The Incident Object Description Exchange Format (IODEF) defines a data representation that provides a framework for sharing information commonly exchanged by Computer Security Incident Response Teams (CSIRTs) about computer security incidents. This document describes the information model for the IODEF and provides an associated data model specified with XML Schema.


```

+-----+
| Indicator |
+-----+
| ENUM restriction | <>-----[ IndicatorID ]
| STRING ext-restriction | <>--{0..*}--[ AlternativeIndicatorID ]
|                   | <>--{0..*}--[ Description ]
|                   | <>--{0..1}--[ StartTime ]
|                   | <>--{0..1}--[ EndTime ]
|                   | <>--{0..1}--[ Confidence ]
|                   | <>--{0..*}--[ Contact ]
|                   | <>--{0..1}--[ Observable ]
|                   | <>--{0..1}--[ ObservableReference ]
|                   | <>--{0..1}--[ IndicatorExpression ]
|                   | <>--{0..1}--[ IndicatorReference ]
|                   | <>--{0..*}--[ NodeRole ]
|                   | <>--{0..*}--[ AttackPhase ]
|                   | <>--{0..*}--[ Reference ]
|                   | <>--{0..*}--[ AdditionalData ]
+-----+

```

Figure 59: The Indicator Class

[[Search](#)] [[txt](#)|[html](#)|[pdf](#)|[bibtex](#)] [[Tracker](#)] [[WG](#)] [[Email](#)] [[Diff1](#)] [[Diff2](#)] [[Nits](#)]
From: [draft-ietf-mile-rolie-16](#) Proposed Standard

Internet Engineering Task Force (IETF)
Request for Comments: 8322
Category: Standards Track
ISSN: 2070-1721

J. Field
Pivotal
S. Banghart
D. Waltermire
NIST
February 2018

Resource-Oriented Lightweight Information Exchange (ROLIE)

Abstract

This document defines a resource-oriented approach for security automation information publication, discovery, and sharing. Using this approach, producers may publish, share, and exchange representations of software descriptors, security incidents, attack indicators, software vulnerabilities, configuration checklists, and other security automation information as web-addressable resources. Furthermore, consumers and other stakeholders may access and search this security information as needed, establishing a rapid and on-demand information exchange network for restricted internal use or public access repositories. This specification extends the Atom Publishing Protocol and Atom Syndication Format to transport and share security automation resource representations.

Status of This Memo

This is an Internet Standards Track document.



Branch: master OpenIOC_1.1 / schemas / ioc.xsd

Find file Copy path

William Gibb Added apache 2.0 license information d42a877 on 8 Aug 2013

1 contributor

Executable File | 125 lines (122 sloc) | 6.02 KB

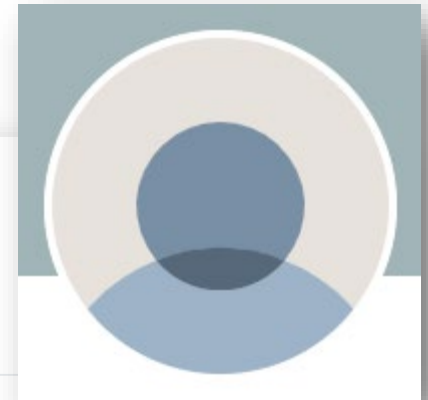
Raw Blame

```
1 <?xml version="1.0" encoding="utf-8"?>
2 <!--
3     TITLE:      OpenIOC 1.1 Schema
4     VERSION:    1.1 (draft)
5     DESCRIPTION: OpenIOC 1.1 Schema document, describing the structure of OpenIOC 1.1.
6     LICENSE:    Copyright 2013 Mandiant Corporation. Licensed under the Apache 2.0 license.
7
8     Mandiant licenses this file to you under the Apache License, Version
9     2.0 (the "License"); you may not use this file except in compliance with the
10    License. You may obtain a copy of the License at:
11
12        http://www.apache.org/licenses/LICENSE-2.0
13
14    Unless required by applicable law or agreed to in writing, software
15    distributed under the License is distributed on an "AS IS" BASIS,
16    WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or
17    implied. See the License for the specific language governing
18    permissions and limitations under the License.
19 -->
```



DDoS Open Threat Signaling (DOTS) Architecture

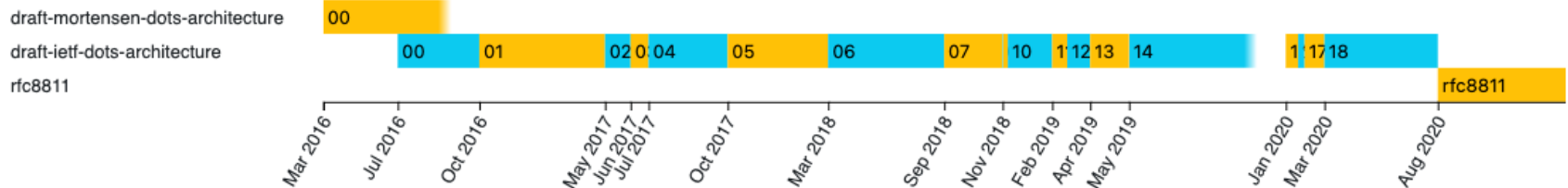
RFC 8811



Status [IESG evaluation record](#) [IESG writeups](#) [Email expansions](#) [History](#)

Versions:

[00](#) [01](#) [02](#) [03](#) [04](#) [05](#) [06](#) [07](#) [08](#) [09](#) [10](#) [11](#) [12](#) [13](#) [14](#) [15](#) [16](#) [17](#) [18](#)



Document	Type	RFC - Informational (August 2020) Was draft-ietf-dots-architecture (dots WG)
	Authors	Andrew Mortensen ✉, Tirumaleswar Reddy.K ✉, Flemming Andreassen ✉, Nik Teague ✉, Rich Compton ✉
	Last updated	2020-08-17





[CVE List](#)

[CNAs](#)

[WGs](#)

[Board](#)

[NVD](#)

[ID Lookup:](#) [Go](#)

[About](#)

[News & Blog](#)

Go to for:

[CVSS Scores](#)

[CPE Info](#)

[Search CVE List](#)

[Downloads](#)

[Data Feeds](#)

[Update a CVE Record](#)



Common Weakness Enumeration

A Community-Developed List of Software & Hardware Weakness Types

NOTICE

NOTICE

[Home](#)

[About](#)

[CWE List](#)

[Scoring](#)

[Mapping Guidance](#)

[Community](#)



[Getting Started](#)

[Releases](#)

[Documentation](#)

[About MAEC](#)

[Community](#)

[En](#)

CVE News

News has moved to the new CVE website.

[Go to CVE News page](#)



Malware Attribute Enumeration and Characterization (MAEC™)

New! MAEC 5.0 now available!

[minutes](#)



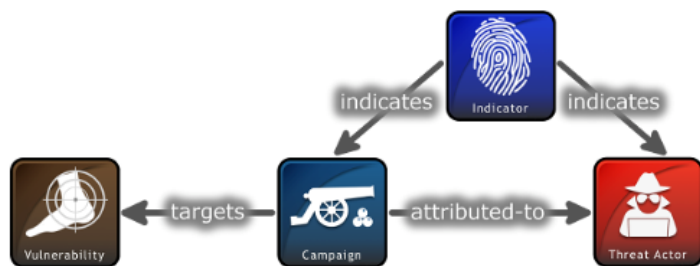


A structured language for cyber threat intelligence

Structured Threat Information Expression (STIX™) is a language and serialization format used to exchange cyber threat intelligence (CTI).

STIX enables organizations to share CTI with one another in a consistent and machine readable manner, allowing security communities to better understand what computer-based attacks they are most likely to see and to anticipate and/or respond to those attacks faster and more effectively.

STIX is designed to improve many different capabilities, such as collaborative threat analysis, automated threat exchange, automated detection and response, and more.



STIX Relationship Example

[🏠 Learn More](#)

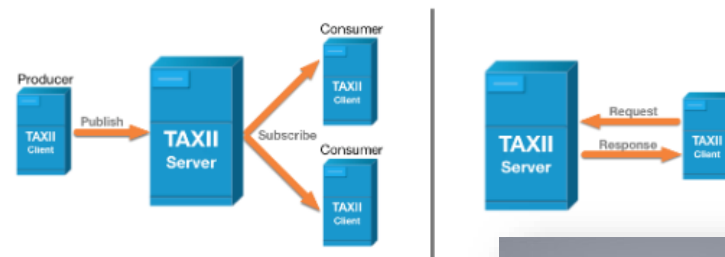


A transport mechanism for sharing cyber threat intelligence

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.

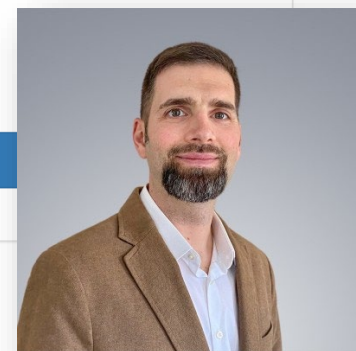
TAXII is a protocol used to exchange cyber threat intelligence (CTI) over HTTPS. TAXII enables organizations to share CTI by defining an API that aligns with common sharing models.

TAXII is specifically designed to support the exchange of CTI represented in STIX.



TAXII Collections

[🏠 Learn More](#)





[Getting Started](#)

[Documentation](#) ▾

[Releases](#) ▾

[Samples](#)

[Community](#) ▾

[About](#)

🔔 This site contains archived CybOX documentation. CybOX has been integrated into STIX 2.0 and STIX 2.0 documentation is available [here](#). STIX is maintained by the **OASIS CTI TC**.

Cyber Observable eXpression (CybOX™) Archive Website

A structured language for cyber observables.

****IMPORTANT NOTICE:**** The CybOX Language has been [integrated](#) into [Version 2.0 of Structured Threat Information eXpression \(STIX™\)](#). Go to the [STIX 2.0 documentation website](#).



[Archived Specification Downloads](#) ↓

[See CybOX Examples](#) »



3. TLP definitions

- a. **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.
- b. **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.**
- c. **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.
- d. **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.





Who do you think you are?

Part two - Organisations



Authorized Users of the CERT Mark

"CERT" is a registered trademark owned by Carnegie Mellon University. CMU has decided to discontinue its practice of licensing the CERT mark internationally. As a result, we will no longer pursue license agreements outside of the United States. Computer security incident response teams (CSIRTs), within the United States, that share the SEI's commitment to improving the security of networks connected to the Internet may apply for authorization to use the "CERT" mark in their names. For those CSIRTs outside of the U.S. CMU recommends that you consult with your own trademark counsel regarding your rights going forward. Should a non-U.S. CSIRT seek to file a trademark application for its own name including "CERT" in the country where it is located (and not the United States), CMU will not oppose the application.

Apply to Use "CERT"

Contact Us

Interested CSIRTs based in the United States must complete and submit a qualification form. **Contact us** to request a form.

Authorized to Use "CERT" Graphic

We created a graphic that authorized CSIRTs can add to their websites.* This graphic provides a visual indication that the CSIRT is part of a network of teams that provide similar services. The graphic indicates that the CSIRT is licensed to use "CERT" in its name; it does not indicate that we endorse or recommend any of the content or services on these sites. Organizations should also adhere to [SEI guidelines](#) for the use of "CERT."

* This seal is for use on the organization's website only; it cannot be used on any other materials.



Authorized to Use CERT™
CERT is a mark owned by
Carnegie Mellon University

This image depicts how AlgoCERT is using the CERT mark on its website.

Click to go forward, hold to see history



Membership

- [Becoming a Member](#) ▾
- [FIRST Teams](#)
- [FIRST Liaisons](#)
- **[Members around the world](#)**

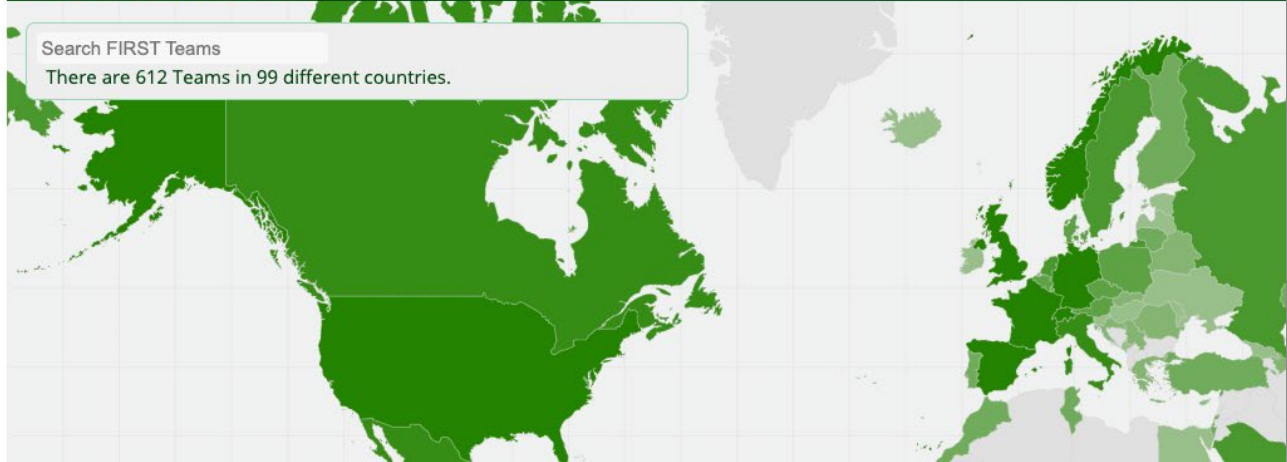
FIRST Teams

View the [complete list and contact information](#) for incident response teams participating in FIRST, the Forum of Incident Response and Security Teams.

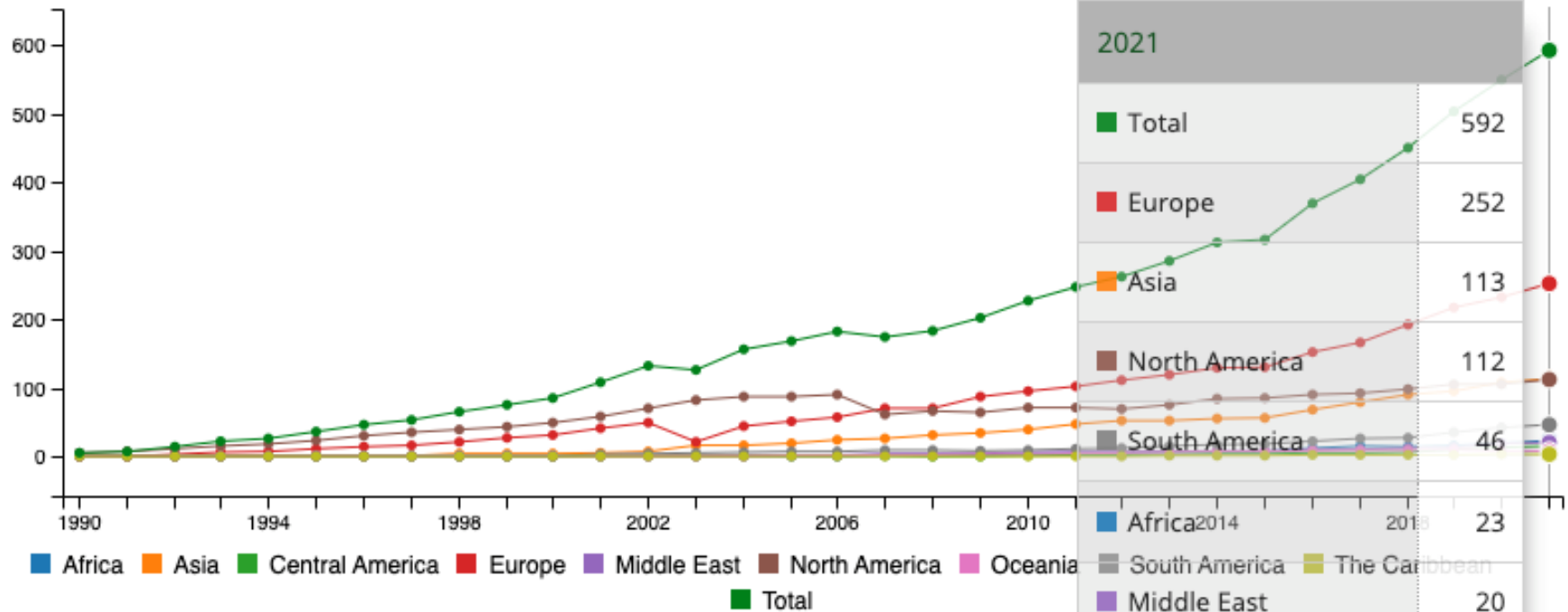
FIRST Members around the world

Search FIRST Teams

There are 612 Teams in 99 different countries.



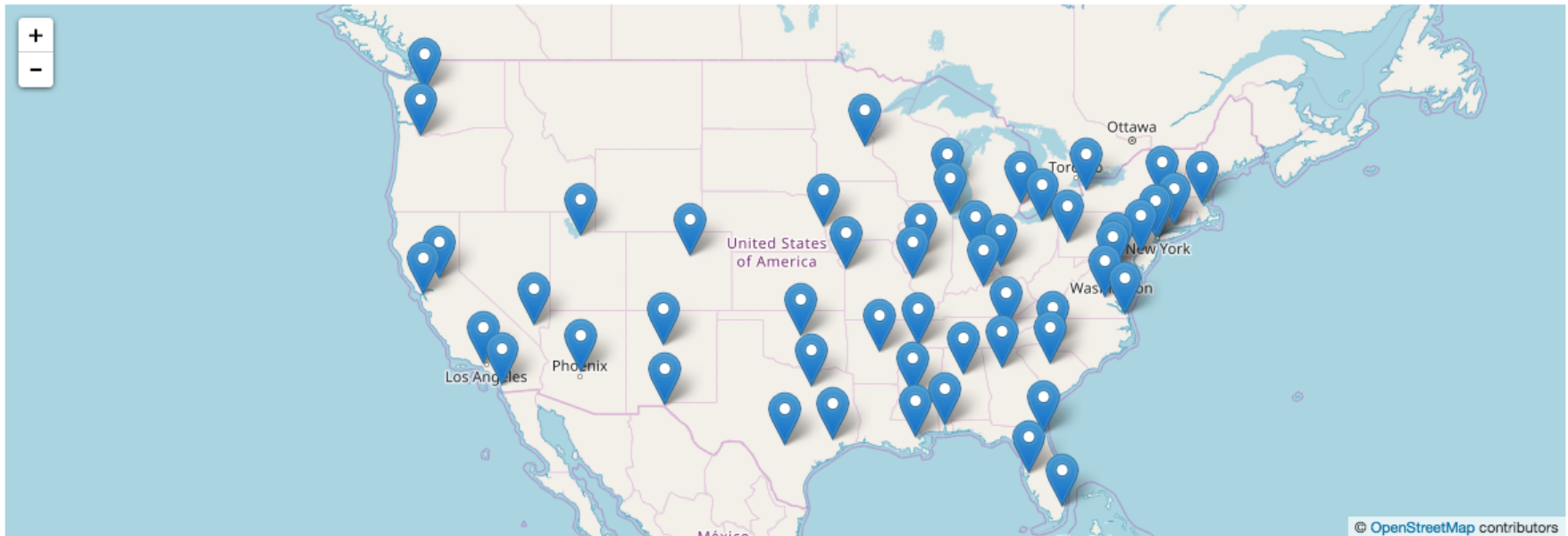
FIRST members growth by year*



(*) The statistic measurement method and regional breakdown changed in 2007



Field Offices



Our local FBI offices are all about protecting your communities.

The FBI has 56 field offices (also called divisions) centrally located in major metropolitan areas across the U.S. and Puerto Rico. They are the places where we carry out investigations, assess local and regional crime threats, and work closely with partners on cases and operations. Each field office is overseen by a special agent in charge, except our offices in Los Angeles, New York City, and Washington, D.C., which are headed by an assistant director in charge due to their large size. Within these field offices are a total of about 380 resident agencies located in smaller cities and towns. Resident agencies are managed by supervisory special agents.



What happened in 1998?

- Clinton - Presidential Decision Directive/NSC-63
- 22 May 1998 “Critical Infrastructure Protection”

“strongly encourage the creation of a private sector information sharing and analysis center [ISAC]”

Information Sharing and Analysis Center (ISAC): The National Coordinator, working with Sector Coordinators, Sector Liaison Officials and the National Economic Council, shall consult with owners and operators of the critical infrastructures to strongly encourage the creation of a private sector information sharing and analysis center. The actual design and functions of the center and its relation to the NIPC will be determined by the private sector, in consultation with and with assistance from the Federal Government. Within 180 days of this directive, the National Coordinator, with the assistance of the CICG including the National Economic Council, shall identify possible methods of providing federal assistance to facilitate the startup of an ISAC.

Such a center could serve as the mechanism for gathering, analyzing, appropriately sanitizing and disseminating private sector information to both industry and the NIPC. The center could also gather, analyze and disseminate information from the NIPC for further distribution to the private sector. While crucial to a successful government-industry partnership, this mechanism for sharing important information about vulnerabilities, threats, intrusions and anomalies is not to interfere with direct information exchanges between companies and the government.

As ultimately designed by private sector representatives, the ISAC may emulate particular aspects of such institutions as the Centers for Disease Control and Prevention that have proved highly effective, particularly its extensive industry participation. Under such a model, the ISAC would possess a large degree of technical focus and expertise and non-regulatory and non-law enforcement missions. It would establish baseline statistics and patterns on the various infrastructures, both among the various sectors, and provide a library for historical data to be used by the private sector and, as deemed appropriate by the ISAC, by the government. Critical to the success of such an institution would be its timeliness, accuracy, and acceptability.



MEMBER ISACS



AMERICAN CHEMISTRY COUNCIL



The American Chemistry Council (ACC) represents a diverse set of companies engaged in the business of chemistry. An innovative, \$553 billion enterprise, our mission is to deliver value to our members through advocacy, member engagement, political advocacy, information sharing, communications and scientific research. The Chemical Information Technology Center (ChemITC®) of the ACC is a forum for companies to address common IT, cyber security, and security issues. Through strategic programs and networking groups dedicated to addressing specific technology issues, ChemITC is committed to advancing the use of information technology to streamline processes, manage cyber threats, and improve decision-making. www.americanchemistry.com/

AUTOMOTIVE ISAC



The Automotive Information Sharing and Analysis Center (Auto-ISAC) is a non-profit information sharing organization that provides a trusted environment and platform for automotive manufacturers and suppliers to collaborate on cybersecurity. Founded by a global group of automakers in 2015, the Auto-ISAC is the central hub for industry-wide sharing of cyber threats, vulnerabilities, and best practices related to the connected vehicle. We embrace a working together model, engaging across the community with automotive strategic partners, trade associations, researchers and universities, and government. Membership is open to light and heavy-duty automotive manufacturers, suppliers, carriers, and fleet operators. www.automotiveisac.com

Membership Benefits

FS-ISAC members around the world receive trusted and timely expert information that increases sector-wide knowledge of physical and cybersecurity threats.

Based on level of service, FS-ISAC members take advantage of a host of important benefits, including early notification of security threats and attacks, anonymous information sharing across the financial services industry, regularly scheduled member meetings and bi-weekly conference calls.

If your firm is not a financial institution, [click here](#) for information on how to participate.

Membership Guidelines

The table below outlines the minimum membership level at which your firm is required to join.

	Core	Standard	Premier	Gold	Platinum
Banks, Credit Unions, Insurance/Reinsurance Companies and Publicly Held Securities/Brokerage Firms	Assets: \$1B - \$10B	Assets: \$10B - \$20B	Assets: \$20B - \$100B	Assets: \$100B - \$250B	Assets: > \$250B
Financial Service Trade Associations, Financial Industry Utilities, Pension Funds, Processors, Utilities and Privately Held Stan	Revenue: < \$100M	Revenue: \$100M - \$1B	Revenue: \$1B - \$2.5B	Revenue: \$2.5B - \$5B	Revenue: > \$5B

Protect your firm and valued customers while taking an active role in safeguarding critical financial infrastructures. Join your peers by becoming a member of FS-ISAC. For more information, please use our membership inquiry form, or contact us at **877-612-2622**.

Compare FS-ISAC Membership Benefits	Core	Standard	Premier	Gold	Platinum
Click to Expand/Collapse all	\$850.00/yr Join Now	\$5,000.00/yr Join Now	\$10,000.00/yr Join Now	\$24,950.00/yr Join Now	\$49,950.00/yr Join Now
+ User Access Credentials	4	10	25	50	Unlimited
+ CINS Crisis Notifications	✓	✓	✓	✓	✓
+ Government, Member, and Partner Alerts	✓	✓	✓	✓	✓
+ Customized Email Notification Profile	✓	✓	✓	✓	✓
+ 24 x 7 Watch Desk	✓	✓	✓	✓	✓
+ Member Submissions	✓	✓	✓	✓	✓
+ Member Surveys	✓	✓	✓	✓	✓
+ Industry Best Practices	✓	✓	✓	✓	✓
+ Member Contact Directory	✓	✓	✓	✓	✓
+ Threat Conference Calls		✓	✓	✓	✓
+ FS-ISAC Committees/Workgroups	✓	✓	✓	✓	✓
+ Number of Free Passes for Member Meetings/Summits			2	5	10
+ XML Data Feeds			✓	✓	✓
+ FS-ISAC Governance				✓	✓

Cyber Obama

- 2013 - Executive Order 13691
 - *“Promoting Private Sector Cybersecurity Information Sharing”*
- 2015 – Cybersecurity Information Sharing Act (CISA)
 - <https://www.congress.gov/bill/114th-congress/senate-bill/754>



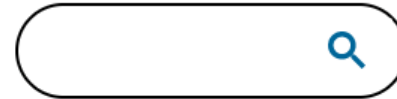
Sec. 2. Information Sharing and Analysis Organizations. (a) The Secretary of Homeland Security (Secretary) shall strongly encourage the development and formation of Information Sharing and Analysis Organizations (ISAOs).

(b) ISAOs may be organized on the basis of sector, sub-sector, region, or any other affinity, including in response to particular emerging threats or vulnerabilities. ISAO membership may be drawn from the public or private sectors, or consist of a combination of public and private sector organizations. ISAOs may be formed as for-profit or nonprofit entities.

(c) The National Cybersecurity and Communications Integration Center (NCCIC), established under section 226(b) of the Homeland Security Act of 2002 (the "Act"), shall engage in continuous, collaborative, and inclusive coordination with ISAOs on the sharing of information related to cybersecurity risks and incidents, addressing such risks and incidents, and strengthening information security systems consistent with sections 212 and 226 of the Act.

(d) In promoting the formation of ISAOs, the Secretary shall consult with other Federal entities responsible for conducting cybersecurity activities, including Sector-Specific Agencies, independent regulatory agencies at their discretion, and national security and law enforcement agencies.





cisa.gov/uscert

[Report Cyber Issue](#)

[Subscribe to Alerts](#)



CYBERSECURITY



INFRASTRUCTURE SECURITY



EMERGENCY COMMUNICATIONS



NATIONAL RISK MANAGEMENT



ABOUT CISA



MEDIA

[Cybersecurity](#) > [Information Sharing](#) > [Cyber Information Sharing and Collaboration Program \(CISCP\)](#)

Information Sharing

[Automated Indicator Sharing \(AIS\)](#)

[Cyber Information Sharing and Collaboration Program \(CISCP\)](#)

[DHS-approved vendors that offer AIS TAXII client compatible certificates](#)

[Enhanced Cybersecurity Services](#)

[Information Sharing and Analysis Organizations](#)

[TLP Definitions and Usage](#)

CYBER INFORMATION SHARING AND COLLABORATION PROGRAM (CISCP)

The U.S. Department of Homeland Security (DHS) Cyber Information Sharing and Collaboration Program (CISCP) enables actionable, relevant, and timely unclassified information exchange through trusted public-private partnerships across all critical infrastructure (CI) sectors. CISCP fosters this collaboration by leveraging the depth and breadth of DHS cybersecurity capabilities within a focused operational context. Through analyst-to-analyst sharing of threat and vulnerability information, CISCP helps partners manage cybersecurity risks and enhances our collective ability to proactively detect, prevent, mitigate, respond to, and recover from cybersecurity incidents. CISCP's overall objective is to build cybersecurity resiliency and to harden the defenses of the United States and its strategic partners.

[Expand All Sections](#)

[Products and Briefings](#) +

[CISA Central Services](#) +





**CYBERSECURITY
& INFRASTRUCTURE
SECURITY AGENCY**


[CISA.gov](#) [Services](#) [Report](#)

[Alerts and Tips](#) [Resources](#)

Homeland Security Information Network

The Cybersecurity and Infrastructure Security Agency (CISA) uses the [Homeland Security Information Network \(HSIN\)](#) to provide a secure, web-based, collaborative system to share sensitive cyber-related information and news with select cybersecurity partners. The CISA Portal on HSIN enables the U.S. Government and its partners to enhance their shared situational awareness on cyber activities by promoting a collaborative workspace for cybersecurity-related discussions.

The Department of Homeland Security (DHS), through CISA, shares threat indicators and advisory information with public, private, and international partners in the network defense community of practice using the CISA Portal, which provides a number of features that enable collaboration and information sharing including:

- A secure messaging capability to allow CISA and its partners to communicate and coordinate during cybersecurity incidents.
- A document library to share documents, files, and indicators of compromise.
- A web conferencing solution for webinars and online meetings.
- A message board for communication and coordination.

To request access, email HSIN.HelpDesk@hq.dhs.gov .



Critical National Infrastructure

Last Updated *20 April 2021*

National Infrastructure are those facilities, systems, sites, information, people, networks and processes, necessary for a country to function and upon which daily life depends. It also includes some functions, sites and organisations which are not critical to the maintenance of essential services, but which need protection due to the potential danger to the public (civil nuclear and chemical sites for example).

In the UK, there are 13 national infrastructure sectors: Chemicals, Civil Nuclear, Communications, Defence, Emergency Services, Energy, Finance, Food, Government, Health, Space, Transport and Water. Several sectors have defined 'sub-sectors'; Emergency Services for example can be split into Police, Ambulance, Fire Services and Coast Guard.

Each sector has one or more Lead Government Department(s) (LGD) responsible for the sector, and ensuring protective security is in place for critical assets.

Not everything within a national infrastructure sector is judged to be 'critical'. The UK government's official definition of CNI is:

'Those critical elements of infrastructure (namely assets, facilities, systems, networks or processes and the essential workers that operate and facilitate them), the loss or compromise of which could result in:

- a) Major detrimental impact on the availability, integrity or delivery of essential services – including those services whose integrity, if compromised, could result in significant loss of life or casualties – taking into account significant economic or social impacts; and/or
- b) Significant impact on national security, national defence, or the functioning of the state.'

CPNI is focussed on providing advice and assistance to those who have responsibility for protecting these most crucial elements of the UK's national infrastructure from national security threats.



UK DIVERSE RESPONSIBILITY FOR SHARING



National Cyber
Security Centre
a part of GCHQ

CPNI

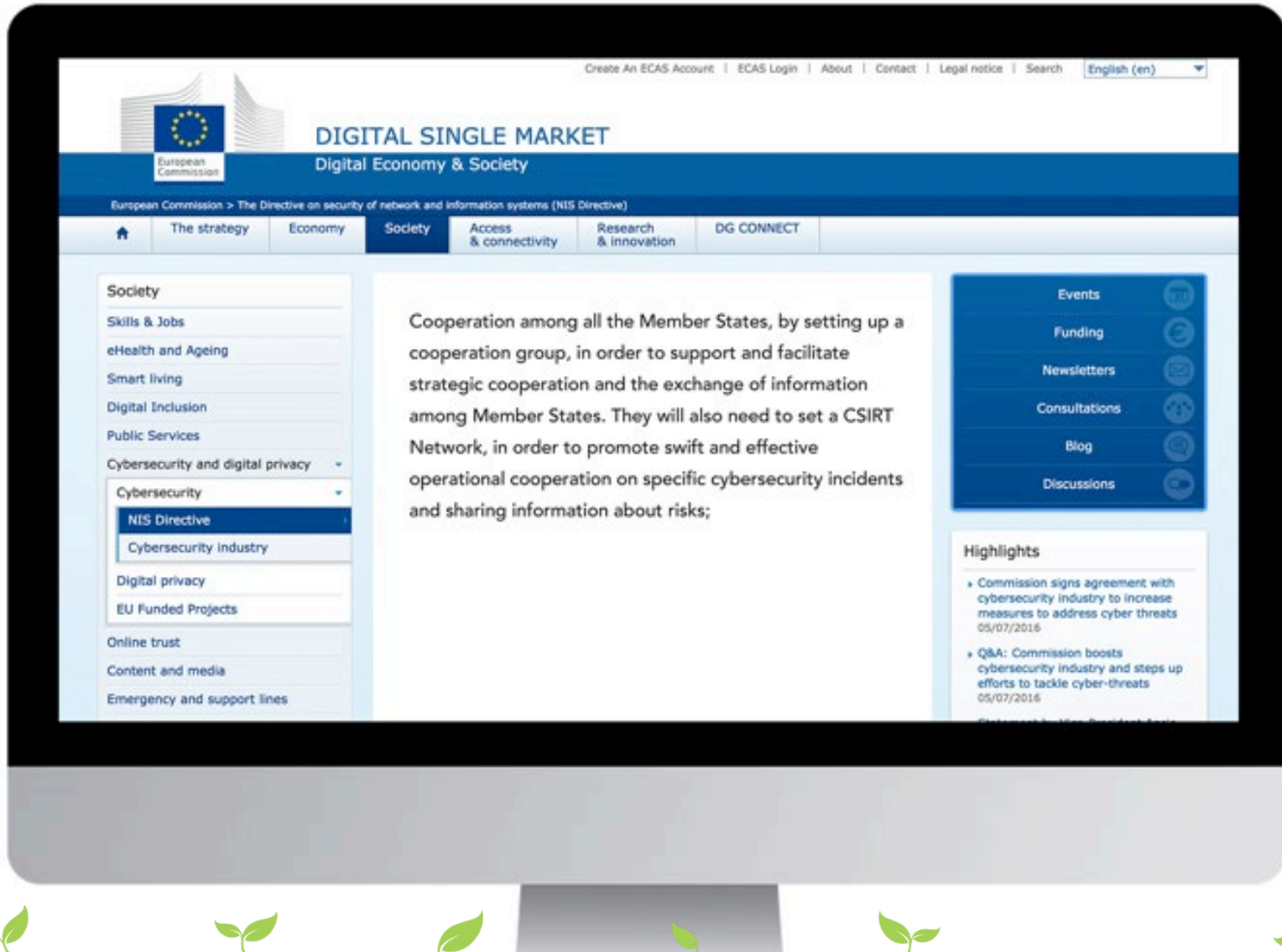
Centre for the Protection
of National Infrastructure



DIB – MANDATORY SHARING



EUROPE NISD



**NEW YORK STATE
DEPARTMENT OF FINANCIAL SERVICES
23 NYCRR 500**

CYBERSECURITY REQUIREMENTS FOR FINANCIAL SERVICES COMPANIES

I, Maria T. Vullo, Superintendent of Financial Services, pursuant to the authority granted by sections 102, 201, 202, 301, 302 and 408 of the Financial Services Law, do hereby promulgate Part 500 of Title 23 of the Official Compilation of Codes, Rules and Regulations of the State of New York, to take effect March 1, 2017, to read as follows:

(ALL MATTER IS NEW)

Section 500.00 Introduction.

The New York State Department of Financial Services (“DFS”) has been closely monitoring the ever-growing threat posed to information and financial systems by nation-states, terrorist organizations and independent criminal actors. Recently, cybercriminals have sought to exploit technological vulnerabilities to gain access to sensitive electronic data. Cybercriminals can cause significant financial losses for DFS regulated entities as well as for New York consumers whose private information may be revealed and/or stolen for illicit purposes. The financial services industry is a significant target of cybersecurity threats. DFS appreciates that many firms have proactively increased their cybersecurity programs with great success.

Given the seriousness of the issue and the risk to all regulated entities, certain regulatory minimum standards are warranted, while not being overly prescriptive so that cybersecurity programs can match the relevant risks and keep pace with technological advances. Accordingly, this regulation is designed to promote the protection of customer information as well as the information technology systems of regulated entities. This regulation requires each company to assess its specific risk profile and design a program that addresses its risks in a robust fashion. Senior management must take this issue seriously and be responsible for the organization’s cybersecurity program and file an annual certification confirming compliance with these regulations. A regulated entity’s cybersecurity program must ensure the safety and soundness of the institution and protect its customers.



Participate | Collaborate | Innovate

