CISA

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA

Greg Park

Law Enforcement Liaison

DHS-CISA Region 9

Greg Park

Law Enforcement Liaison

DHS-CISA Region 9

30+ years Local Government
Public Safety / EMT
Law Enforcement
Information Technology / Cyber

Introduction to CISA

Introduction to CISA

Mission

Introduction to CISA

Mission

Regional Structure

Introduction to CISA

Mission

Regional Structure

Services

Introduction to CISA

Mission

Regional Structure

Services

Notifications

Introduction to CISA

Mission

Regional Structure

Services

Notifications

A.I. Trends

Introduction to CISA

- Mission
- Regional Structure
- Services
- Notifications
- A.I. Trends

Take Aways

Executive

Legislative

Judicial

CISA | CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Executive

CISA

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Executive

CISA

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Federal Law Enforcement Training Centers

Science and Technology Directorate

Office of Intelligence and Analysis

Office of Strategy, Policy, and Plans

Office of the General Counsel

Office of Inspector General

Office for State and Local Law Enforcement

Office of Homeland Security Situational Awareness

Office of Partnership and Engagement

Countering Weapons of Mass Destruction Office

Office of Legislative Affairs

Office of Public Affairs

Privacy Office

Office of the Immigration Detention Ombudsman

Office of the Citizenship and Immigration Services Ombudsman

Office for Civil Rights and Civil Liberties

Office of Health Security

U.S. Immigration and Customs Enforcement

U.S. Customs and Border Protection

U.S. Citizenship and Immigration Services

Federal Emergency Management Agency

U.S. Secret Service

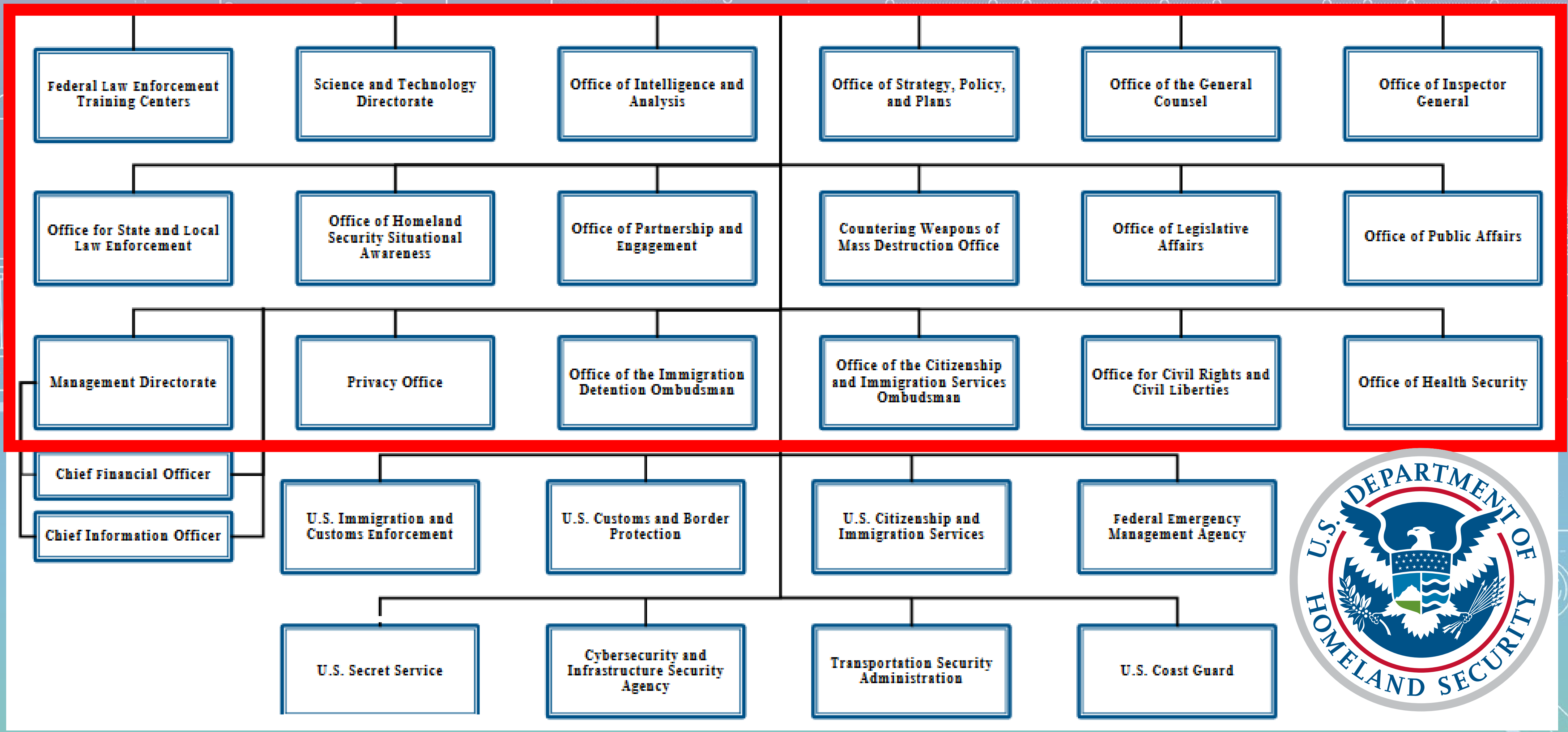
Cybersecurity and Infrastructure Security Agency

Transportation Security Administration

U.S. Coast Guard

Kristi Noem

8th DHS Secretary



Federal Law Enforcement Training Centers

Science and Technology Directorate

Office of Intelligence and Analysis

Office of Strategy, Policy, and Plans

Office of the General Counsel

Office of Inspector General

Office for State and Local Law Enforcement

Office of Homeland Security Situational Awareness

Office of Partnership and Engagement

Countering Weapons of Mass Destruction Office

Office of Legislative Affairs

Office of Public Affairs

Management Directorate

Privacy Office

Office of the Immigration Detention Ombudsman

Office of the Citizenship and Immigration Services Ombudsman

Office for Civil Rights and Civil Liberties

Office of Health Security

Chief Financial Officer

Chief Information Officer

U.S. Immigration and Customs Enforcement

U.S. Customs and Border Protection

U.S. Citizenship and Immigration Services

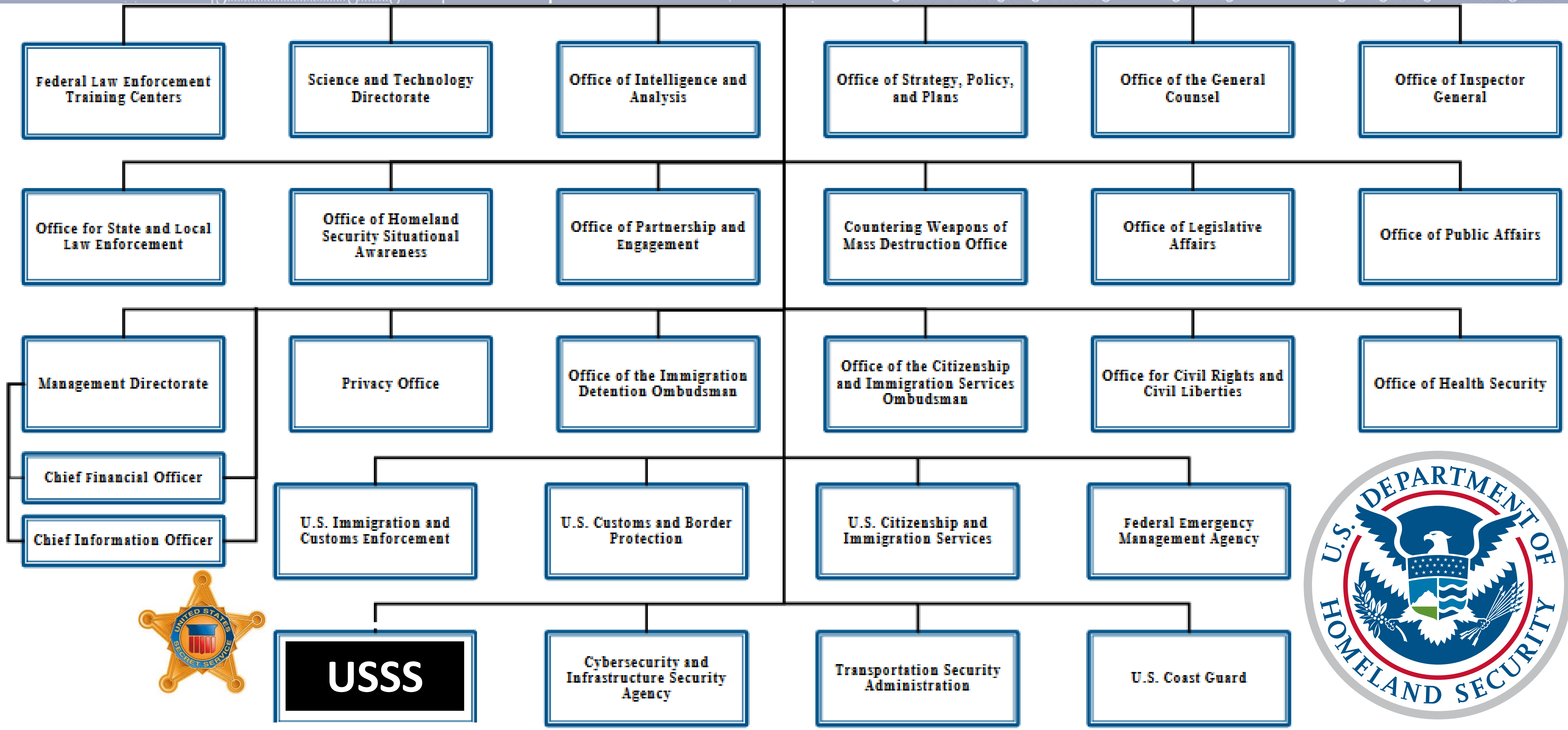
Federal Emergency Management Agency

U.S. Secret Service

Cybersecurity and Infrastructure Security Agency

Transportation Security Administration

U.S. Coast Guard



Federal Law Enforcement Training Centers

Science and Technology Directorate

Office of Intelligence and Analysis

Office of Strategy, Policy, and Plans

Office of the General Counsel

Office of Inspector General

Office for State and Local Law Enforcement

Office of Homeland Security Situational Awareness

Office of Partnership and Engagement

Countering Weapons of Mass Destruction Office

Office of Legislative Affairs

Office of Public Affairs

Management Directorate

Privacy Office

Office of the Immigration Detention Ombudsman

Office of the Citizenship and Immigration Services Ombudsman

Office for Civil Rights and Civil Liberties

Office of Health Security

Chief Financial Officer

Chief Information Officer

U.S. Immigration and Customs Enforcement

U.S. Customs and Border Protection

U.S. Citizenship and Immigration Services

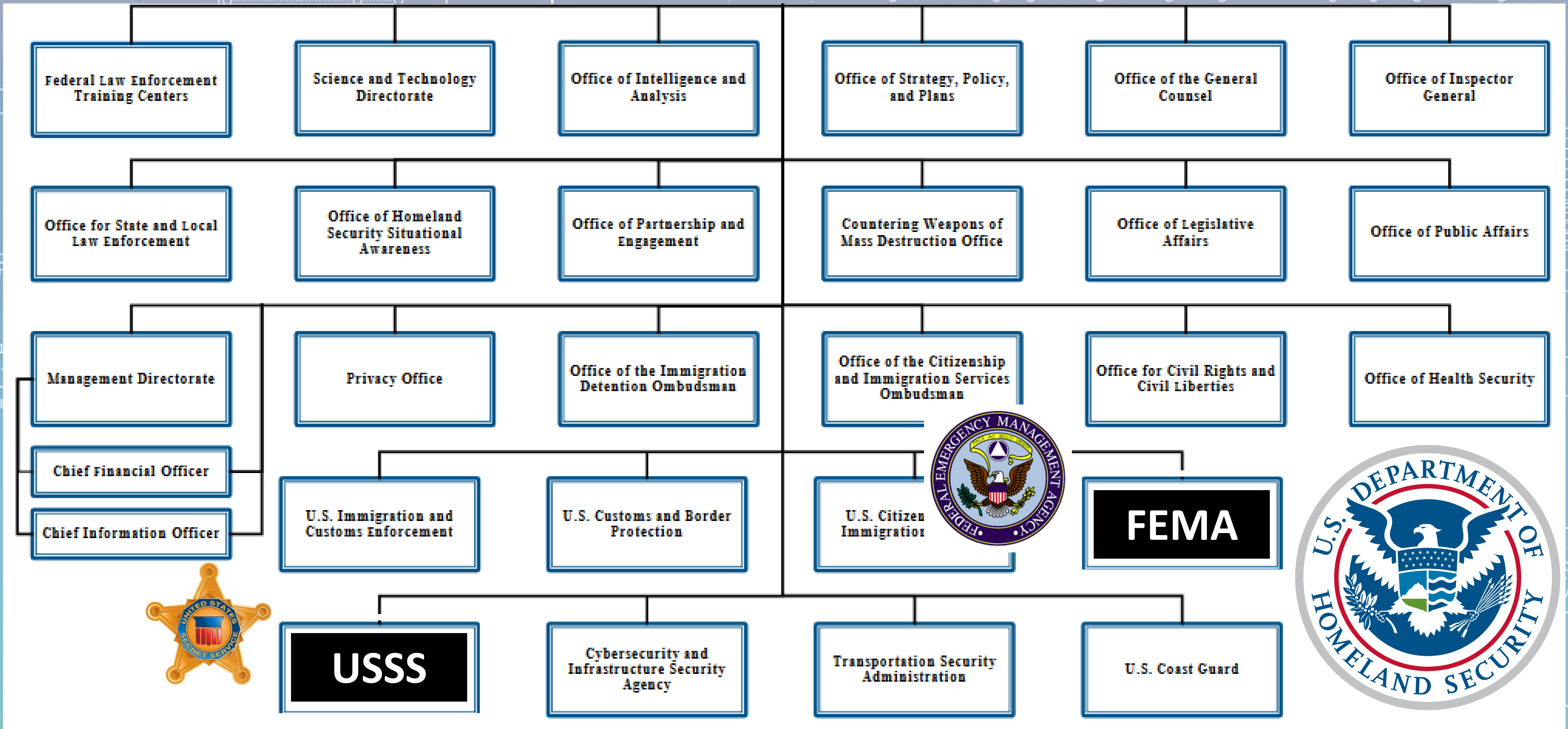
Federal Emergency Management Agency

USSS

Cybersecurity and Infrastructure Security Agency

Transportation Security Administration

U.S. Coast Guard



Federal Law Enforcement Training Centers

Science and Technology Directorate

Office of Intelligence and Analysis

Office of Strategy, Policy, and Plans

Office of the General Counsel

Office of Inspector General

Office for State and Local Law Enforcement

Office of Homeland Security Situational Awareness

Office of Partnership and Engagement

Countering Weapons of Mass Destruction Office

Office of Legislative Affairs

Office of Public Affairs

Management Directorate

Chief Financial Officer

Chief Information Officer

Privacy Office

Office of the Immigration Detention Ombudsman

Office of the Citizenship and Immigration Services Ombudsman

Office for Civil Rights and Civil Liberties

Office of Health Security

U.S. Immigration and Customs Enforcement

U.S. Customs and Border Protection

U.S. Citizen

Immigratior

FEMA

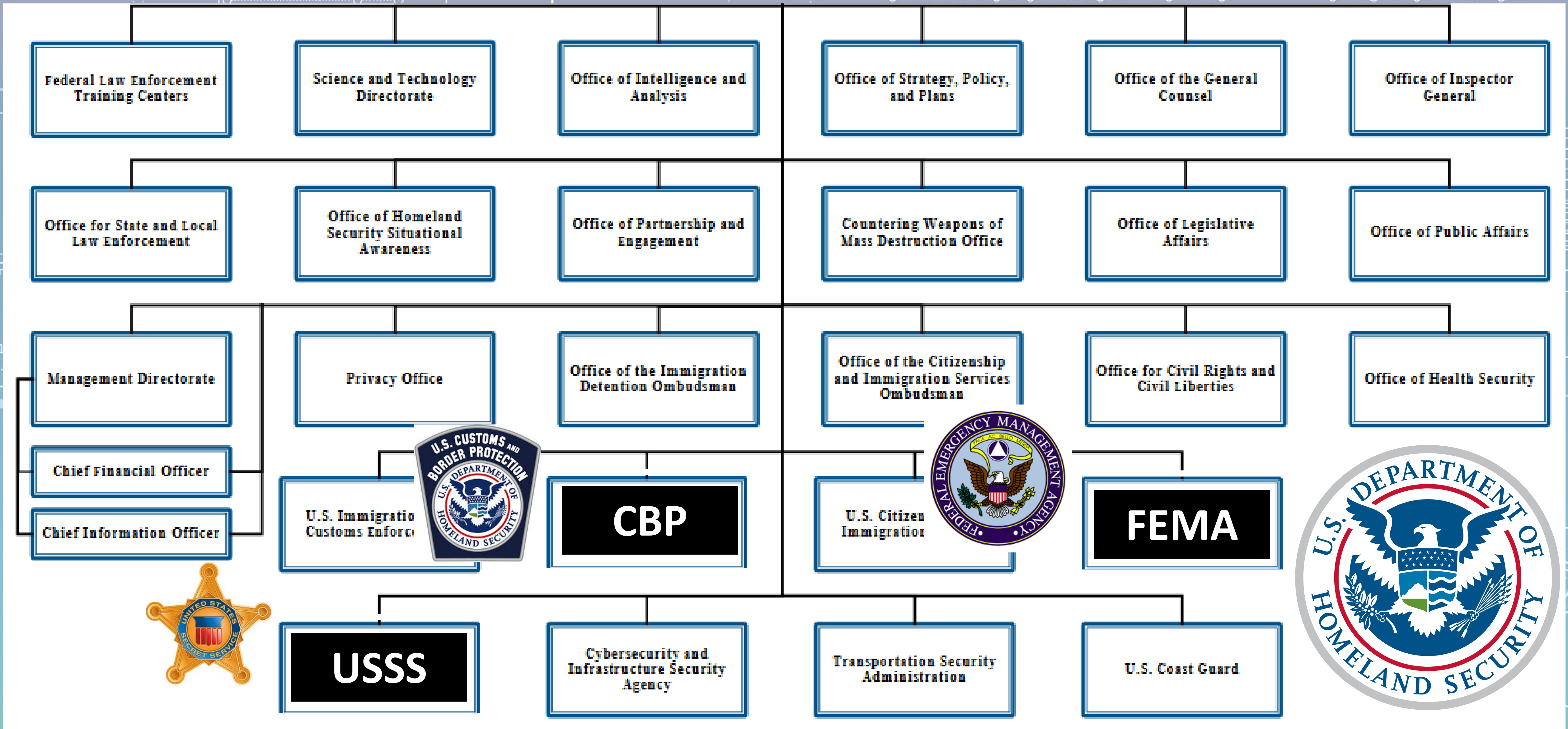
USSS

Cybersecurity and Infrastructure Security Agency

Transportation Security Administration

U.S. Coast Guard

FEDERAL EMERGENCY MANAGEMENT AGENCY
UNITED STATES SECRET SERVICE
U.S. DEPARTMENT OF HOMELAND SECURITY



Federal Law Enforcement Training Centers

Science and Technology Directorate

Office of Intelligence and Analysis

Office of Strategy, Policy, and Plans

Office of the General Counsel

Office of Inspector General

Office for State and Local Law Enforcement

Office of Homeland Security Situational Awareness

Office of Partnership and Engagement

Countering Weapons of Mass Destruction Office

Office of Legislative Affairs

Office of Public Affairs

Management Directorate

Privacy Office

Office of the Immigration Detention Ombudsman

Office of the Citizenship and Immigration Services Ombudsman

Office for Civil Rights and Civil Liberties

Office of Health Security

Chief Financial Officer

Chief Information Officer

U.S. Immigratio Customs Enforc

CBP

U.S. Citizen Immigratior

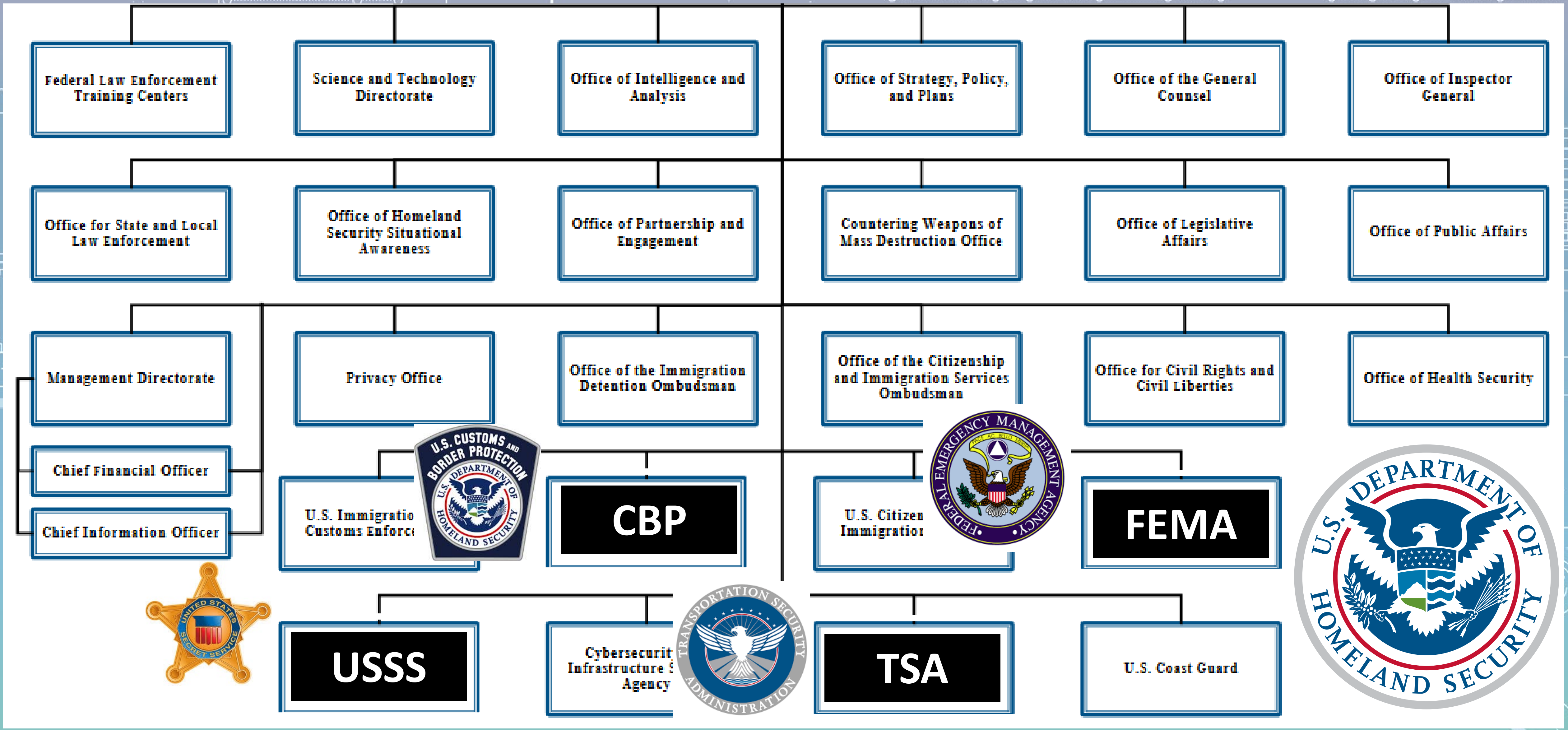
FEMA

USSS

Cybersecurity and Infrastructure Security Agency

Transportation Security Administration

U.S. Coast Guard



Federal Law Enforcement Training Centers

Science and Technology Directorate

Office of Intelligence and Analysis

Office of Strategy, Policy, and Plans

Office of the General Counsel

Office of Inspector General

Office for State and Local Law Enforcement

Office of Homeland Security Situational Awareness

Office of Partnership and Engagement

Countering Weapons of Mass Destruction Office

Office of Legislative Affairs

Office of Public Affairs

Management Directorate

Privacy Office

Office of the Immigration Detention Ombudsman

Office of the Citizenship and Immigration Services Ombudsman

Office for Civil Rights and Civil Liberties

Office of Health Security

Chief Financial Officer

Chief Information Officer

U.S. Immigratio Customs Enforc

CBP

U.S. Citizen Immigratior

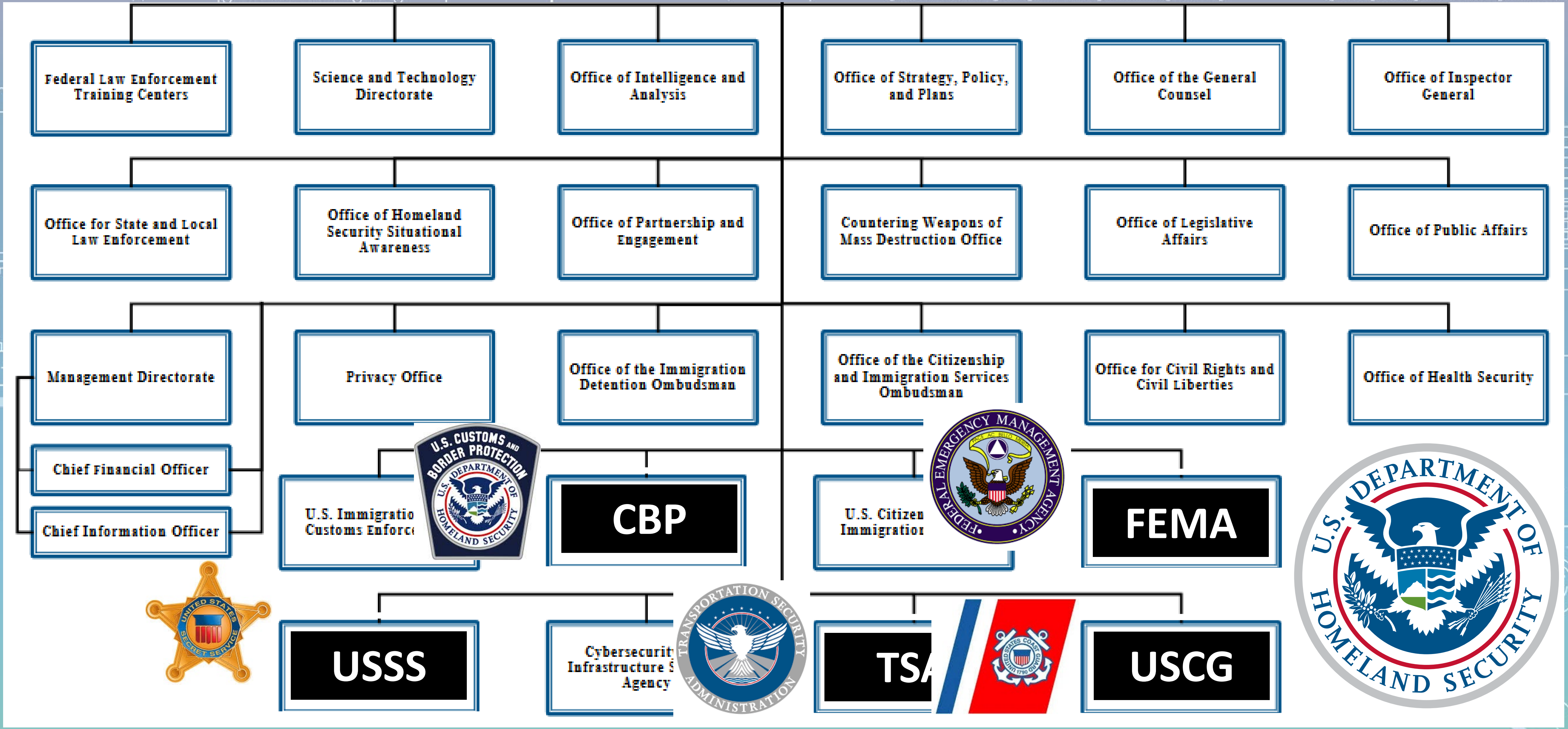
FEMA

USSS

Cybersecurity Infrastructure S Agency

TSA

U.S. Coast Guard



Federal Law Enforcement Training Centers

Science and Technology Directorate

Office of Intelligence and Analysis

Office of Strategy, Policy, and Plans

Office of the General Counsel

Office of Inspector General

Office for State and Local Law Enforcement

Office of Homeland Security Situational Awareness

Office of Partnership and Engagement

Countering Weapons of Mass Destruction Office

Office of Legislative Affairs

Office of Public Affairs

Management Directorate

Privacy Office

Office of the Immigration Detention Ombudsman

Office of the Citizenship and Immigration Services Ombudsman

Office for Civil Rights and Civil Liberties

Office of Health Security

Chief Financial Officer

Chief Information Officer

U.S. Immigratio Customs Enforc

CBP

U.S. Citizen Immigratior

FEMA

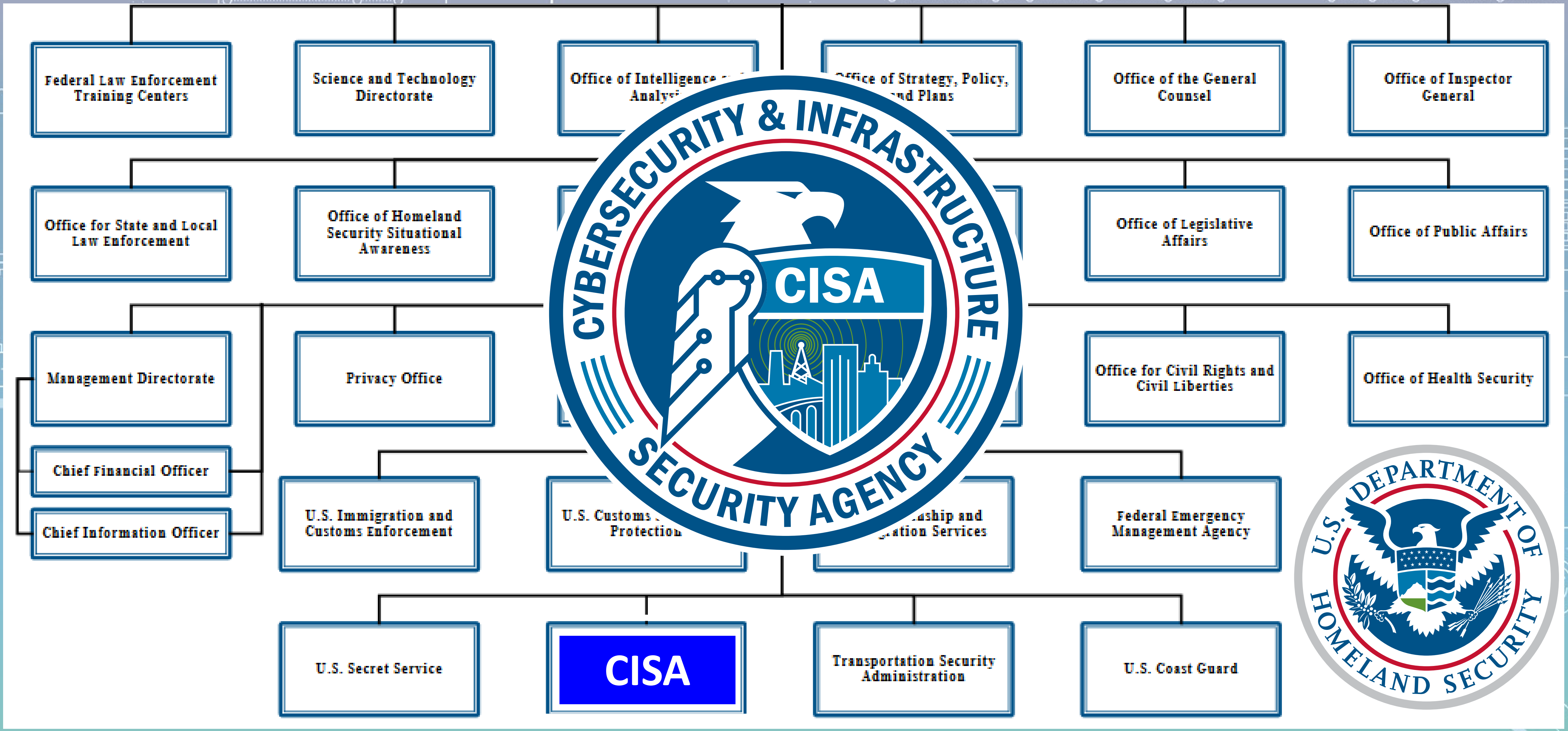
USSS

Cybersecurit Infrastructure S Agency

TSA

USCG

U.S. CUSTOMS AND BORDER PROTECTION
FEDERAL EMERGENCY MANAGEMENT AGENCY
UNITED STATES SECRET SERVICE
TRANSPORTATION SECURITY ADMINISTRATION
U.S. DEPARTMENT OF HOMELAND SECURITY



Federal Law Enforcement Training Centers

Science and Technology Directorate

Office of Intelligence
Analysi

ffice of Strategy, Policy,
nd Plans

Office of the General Counsel

Office of Inspector General

Office for State and Local Law Enforcement

Office of Homeland Security Situational Awareness

Office of Legislative Affairs

Office of Public Affairs

Management Directorate

Chief Financial Officer

Chief Information Officer

Privacy Office

Office for Civil Rights and Civil Liberties

Office of Health Security

U.S. Immigration and Customs Enforcement

U.S. Customs
Protection

nship and
ation Services

Federal Emergency Management Agency

U.S. Secret Service

CISA

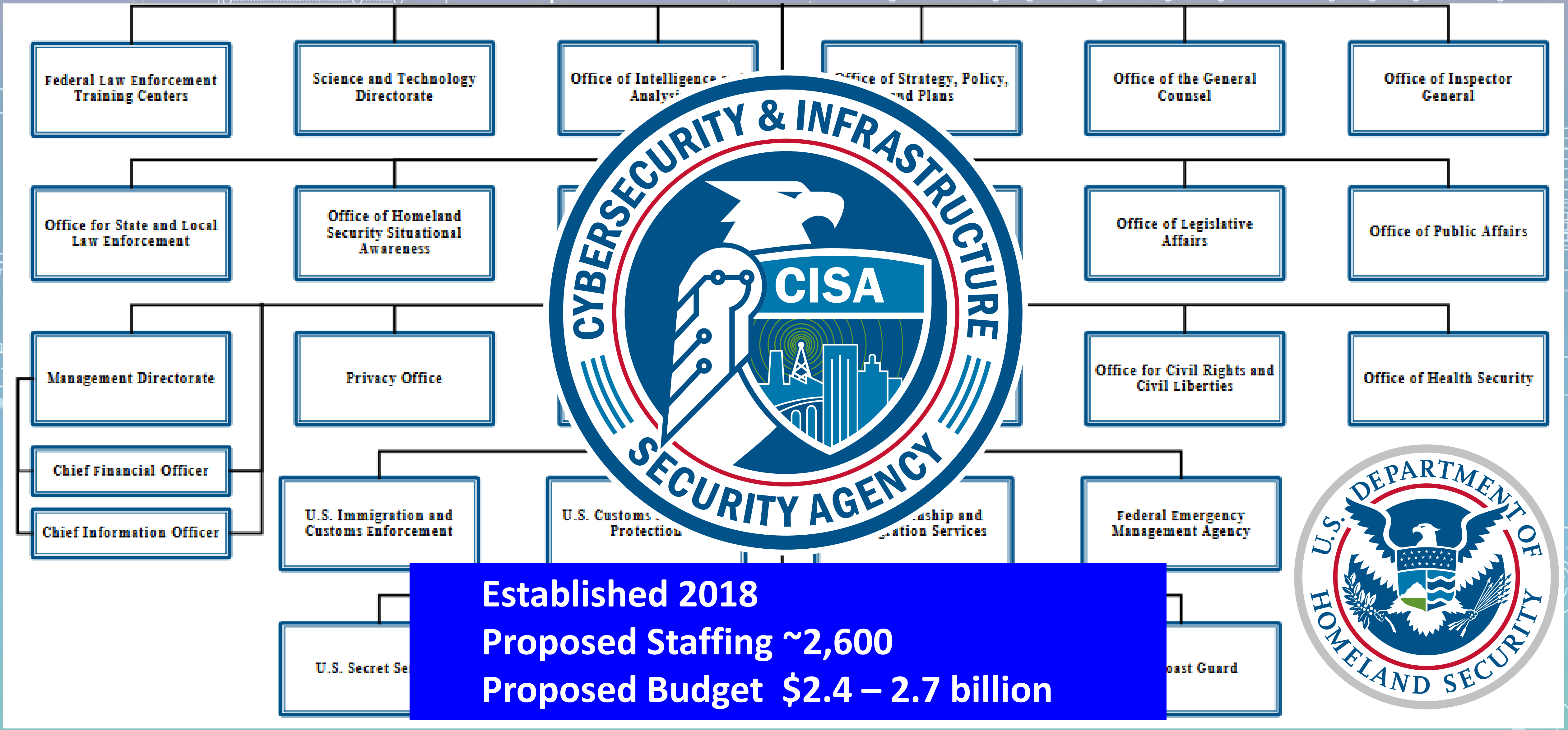
Transportation Security Administration

U.S. Coast Guard

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA

U.S. DEPARTMENT OF HOMELAND SECURITY



Federal Law Enforcement Training Centers

Science and Technology Directorate

Office of Intelligence
Analysi

ffice of Strategy, Policy,
nd Plans

Office of the General Counsel

Office of Inspector General

Office for State and Local Law Enforcement

Office of Homeland Security Situational Awareness

Office of Legislative Affairs

Office of Public Affairs

Management Directorate

Chief Financial Officer

Chief Information Officer

Privacy Office

Office for Civil Rights and Civil Liberties

Office of Health Security

U.S. Immigration and Customs Enforcement

U.S. Customs
Protection

nship and
ation Services

Federal Emergency Management Agency

U.S. Secret Se

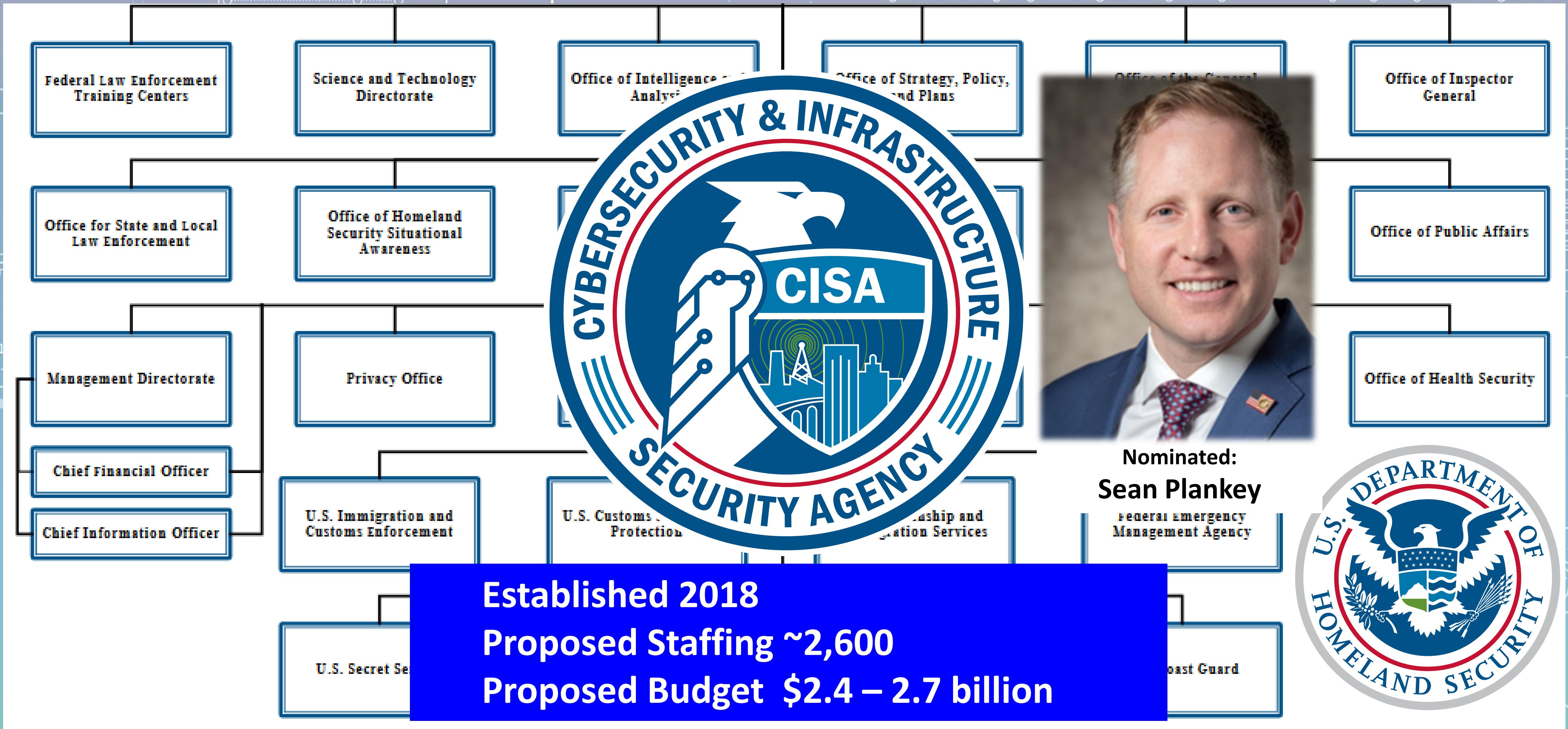
oast Guard

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA

U.S. DEPARTMENT OF HOMELAND SECURITY

Established 2018
Proposed Staffing ~2,600
Proposed Budget $2.4 – 2.7 billion



Federal Law Enforcement Training Centers

Science and Technology Directorate

Office of Intelligence a
Analysi

ffice of Strategy, Policy,
nd Plans

Office of the General

Office of Inspector General

Office for State and Local Law Enforcement

Office of Homeland Security Situational Awareness

Office of Public Affairs

Management Directorate

Privacy Office

Office of Health Security

Chief Financial Officer

Chief Information Officer

U.S. Immigration and Customs Enforcement

U.S. Customs
Protection

ship and
ation Services

Federal Emergency Management Agency

U.S. Secret Se

oast Guard

Nominated:
Sean Plankey

Established 2018
Proposed Staffing ~2,600
Proposed Budget $2.4 – 2.7 billion

Cybersecurity and Infrastructure Security Agency (CISA)

The Nation’s Risk Manager

As America’s Cyber Defense Agency and the National Coordinator for Critical Infrastructure Security and Resilience, CISA leads the national effort to understand, manage, and reduce risk to the cyber and physical infrastructure that Americans rely on every hour of every day.

Mission

Cybersecurity and Infrastructure Security Agency (CISA)

The Nation's Risk Manager

As America's Cyber Defense Agency and the National Coordinator for Critical Infrastructure Security and Resilience, CISA leads the national effort to understand, manage, and reduce risk to the cyber and physical infrastructure that Americans rely on every hour of every day.

➡ Not Tasked with Regulatory or Investigative Powers

Mission

Cybersecurity and Infrastructure Security Agency (CISA)

The Nation’s Risk Manager

As America’s Cyber Defense Agency and the National Coordinator for Critical Infrastructure Security and Resilience, CISA leads the national effort to understand, manage, and reduce risk to the cyber and physical infrastructure that Americans rely on every hour of every day.

Not Tasked with Regulatory or Investigative Powers

➡ Privacy Protections covered under the CISA Act of 2015

Mission

16 Critical Infrastructure Sectors & Corresponding Sector Risk Management Agencies

CHEMICAL	CISA
COMMERCIAL FACILITIES	CISA
COMMUNICATIONS	CISA
CRITICAL MANUFACTURING	CISA
DAMS	CISA
DEFENSE INDUSTRIAL BASE	DOD
EMERGENCY SERVICES	CISA
ENERGY	DOE
FINANCIAL	Treasury
FOOD & AGRICULTURE	USDA & HHS
GOVERNMENT FACILITIES	GSA & FPS
HEALTHCARE & PUBLIC HEALTH	HHS
INFORMATION TECHNOLOGY	CISA
NUCLEAR REACTORS, MATERIALS AND WASTE	CISA
TRANSPORTATIONS SYSTEMS	TSA & USCG
WATER	EPA

Mission

16 Critical Infrastructure Sectors & Corresponding Sector Risk Management Agencies

CHEMICAL	CISA
COMMERCIAL FACILITIES	CISA
COMMUNICATIONS	CISA
CRITICAL MANUFACTURING	CISA
DAMS	CISA
DEFENSE INDUSTRIAL BASE	DOD
EMERGENCY SERVICES	CISA
ENERGY	DOE
FINANCIAL	Treasury
FOOD & AGRICULTURE	USDA & HHS
GOVERNMENT FACILITIES	GSA & FPS
HEALTHCARE & PUBLIC HEALTH	HHS
INFORMATION TECHNOLOGY	CISA
NUCLEAR REACTORS, MATERIALS AND WASTE	CISA
TRANSPORTATIONS SYSTEMS	TSA & USCG
WATER	EPA

Mission

16 Critical Infrastructure Sectors & Corresponding Sector Risk Management Agencies

CHEMICAL	CISA
EMERGENCY SERVICES	CISA
ENERGY	DOE
FINANCIAL	Treasury
FOOD & AGRICULTURE	USDA & HHS
GOVERNMENT FACILITIES	GSA & FPS
HEALTHCARE & PUBLIC HEALTH	HHS
INFORMATION TECHNOLOGY	CISA
NUCLEAR REACTORS, MATERIALS AND WASTE	CISA
TRANSPORTATIONS SYSTEMS	TSA & USCG
WATER	EPA

Mission

16 Critical Infrastructure Sectors & Corresponding Sector Risk Management Agencies

CHEMICAL CISA

FINANCIA

OOD & GRICULT

GOVERNM ACILITIES

IEALTHCA UBLIC HE

NFORMAT ECHNOLO

IUCLEAR IATERIAL

EMERGENCY SERVICES CISA

TRANSPO SYSTEMS

ENERGY DOE

WATER EPA

Mission

16 Critical Infra rresponding
Sector R cies

CHEMICAL

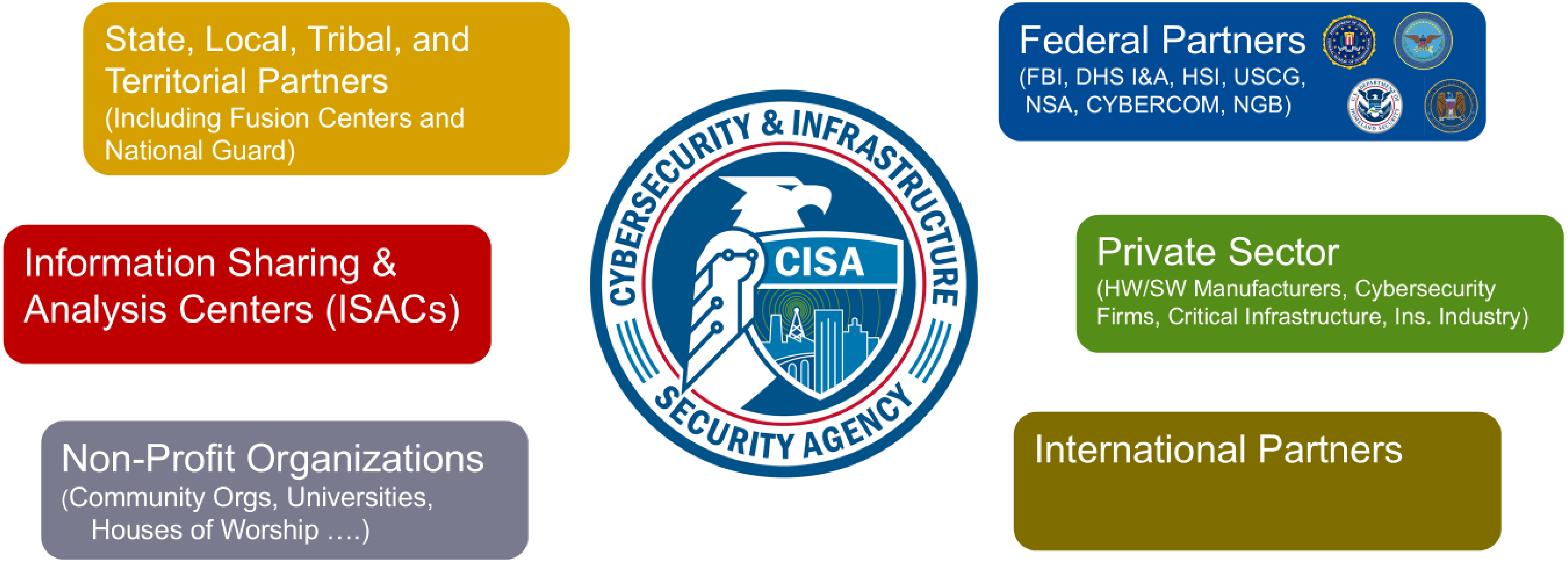
EMERGENCY
SERVICES

ENERGY

EPA

Mission

Cybersecurity Partner Environment



State, Local, Tribal, and Territorial Partners (Including Fusion Centers and National Guard)

Information Sharing & Analysis Centers (ISACs)

Non-Profit Organizations (Community Orgs, Universities, Houses of Worship ….)

Federal Partners (FBI, DHS I&A, HSI, USCG, NSA, CYBERCOM, NGB)

Private Sector (HW/SW Manufacturers, Cybersecurity Firms, Critical Infrastructure, Ins. Industry)

International Partners

Mission

Cybersecurity Partner Environment

State, Local, Tribal, and Territorial Partners
(Including Fusion Centers and National Guard)

Information Sharing & Analysis Centers (ISACs)

Non-Profit Organizations
(Community Orgs, Universities, Houses of Worship ….)

Federal Partners
(FBI, DHS I&A, HSI, USCG, NSA, CYBERCOM, NGB)

Private Sector
(HW/SW Manufacturers, Cybersecurity Firms, Critical Infrastructure, Ins. Industry)

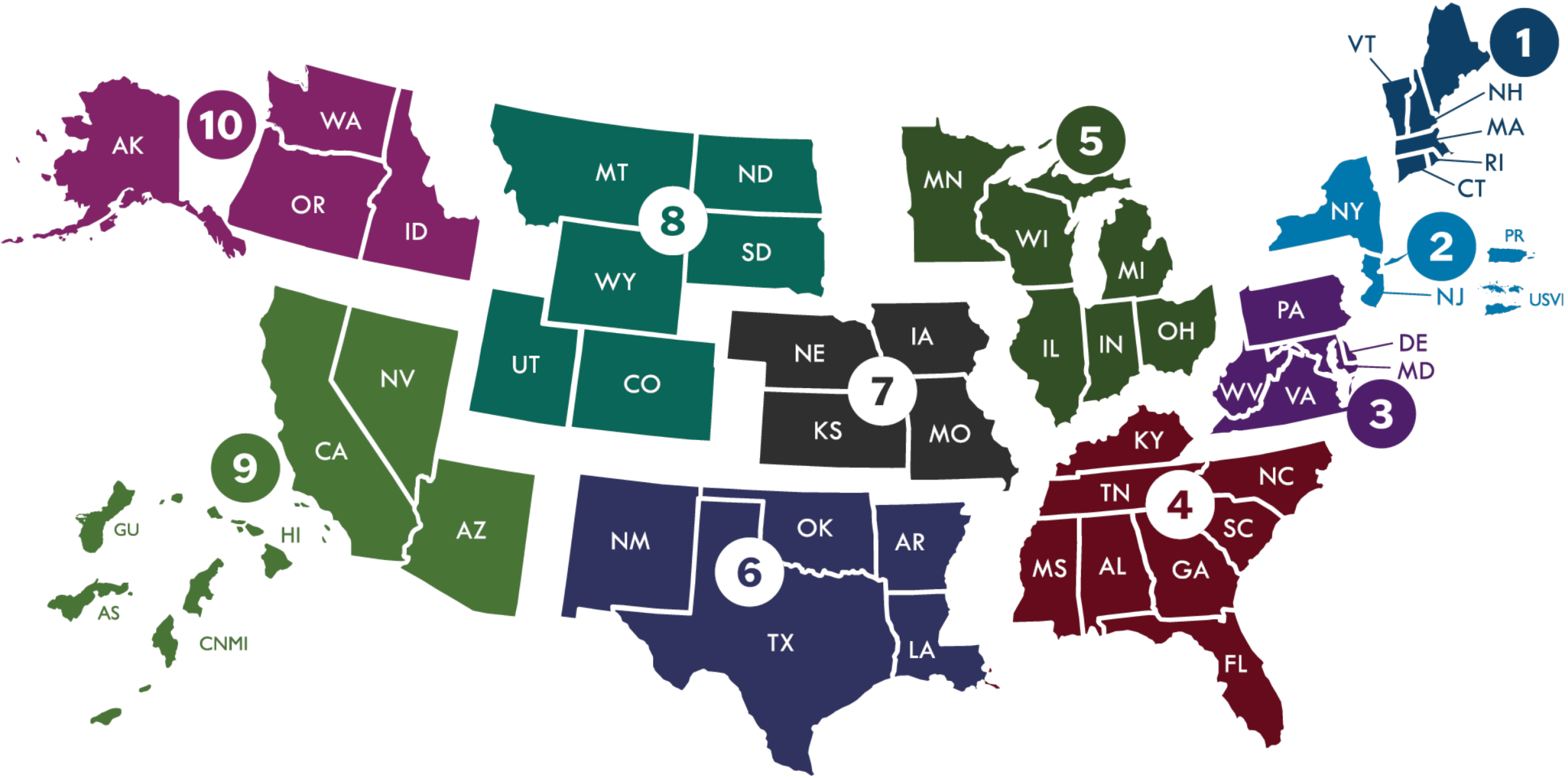
International Partners

Your Organizations

Mission

CISA Regions

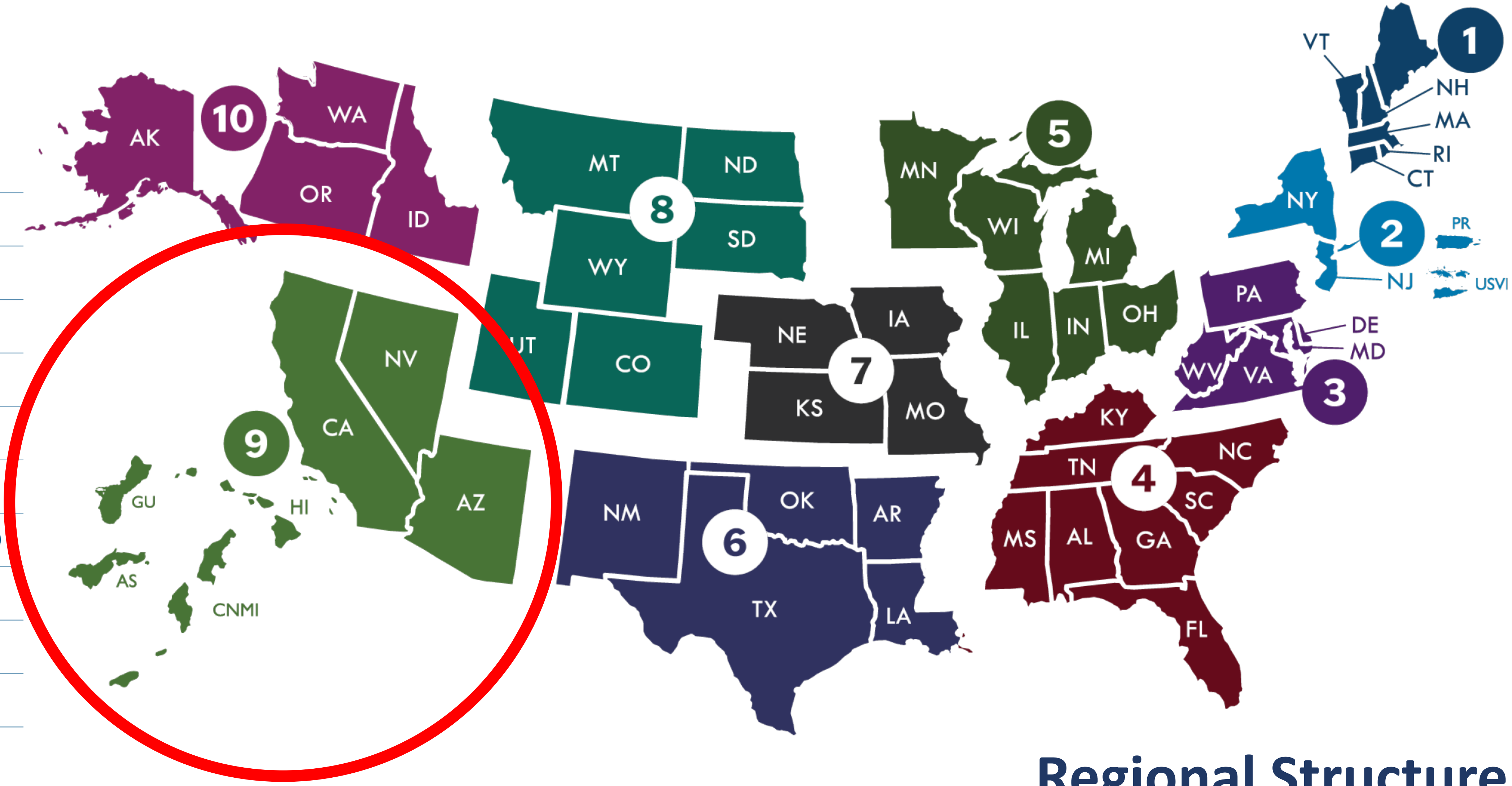
1	Boston, MA
2	New York, NY
3	Philadelphia, PA
4	Atlanta, GA
5	Chicago, IL
6	Dallas, TX
7	Kansas City, MO
8	Denver, CO
9	Oakland, CA
10	Seattle, WA



Regional Structure

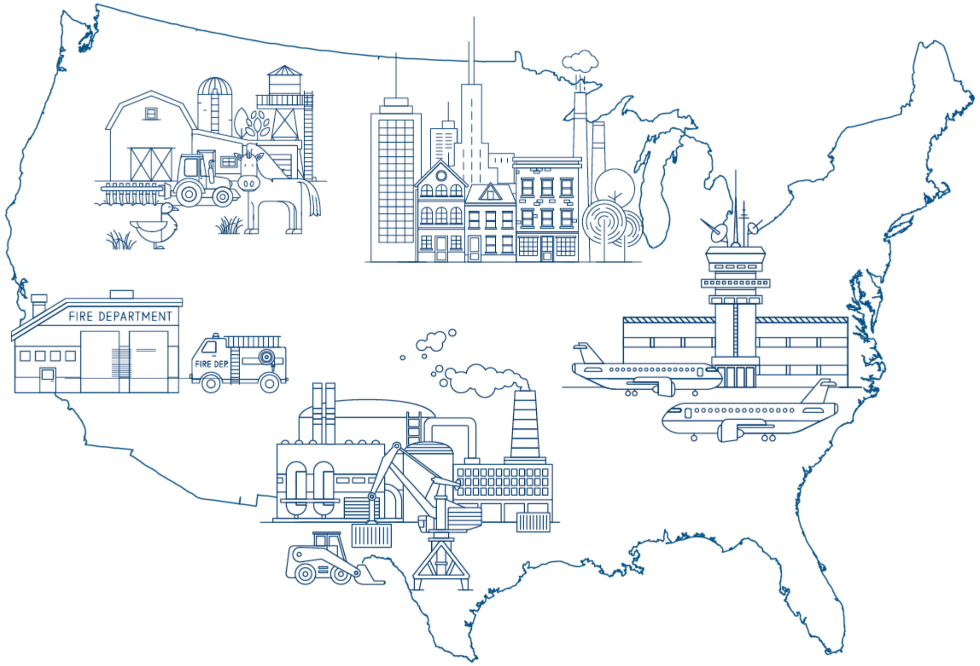
CISA Regions

1	Boston, MA
2	New York, NY
3	Philadelphia, PA
4	Atlanta, GA
5	Chicago, IL
6	Dallas, TX
7	Kansas City, MO
8	Denver, CO
9	Oakland, CA
10	Seattle, WA



Regional Structure

Integrated Operations



I.O.D.

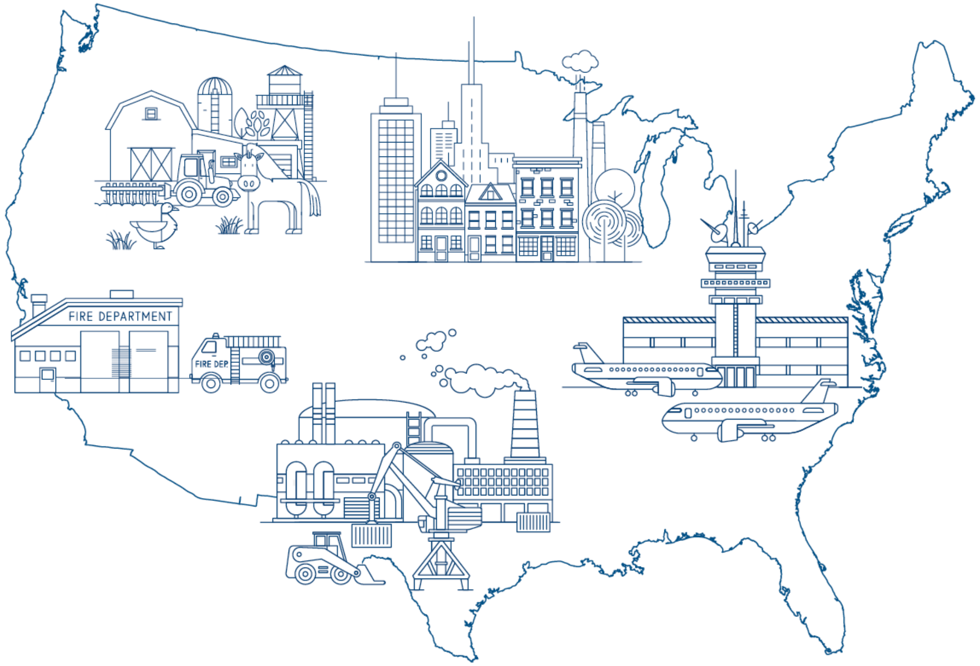
CISA's Integrated Operations Division enhances the resilience of our nation's critical infrastructure by taking an integrated approach to delivering services and sharing information. By meeting our stakeholders where they are, we help critical infrastructure owners and operators mitigate risk.

HOW CISA IS CARRYING OUT ITS INTEGRATED OPERATIONS MISSION:

- Provide Operational Visibility to Understand, Manage, and Reduce Risk to the Nation
- Offer a Unified Regional Approach to Sharing Information and Delivering CISA Services

ZERO COST

Integrated Operations



I.O.D.

CISA's Integrated Operations Division enhances the resilience of our nation's critical infrastructure by taking an integrated approach to delivering services and sharing information. By meeting our stakeholders where they are, we help critical infrastructure owners and operators mitigate risk.

HOW CISA IS CARRYING OUT ITS INTEGRATED OPERATIONS MISSION:

- Provide Operational Visibility to Understand, Manage, and Reduce Risk to the Nation
- Offer a Unified Regional Approach to Sharing Information and Delivering CISA Services

Protective Security Advisors

SURVEYS AND ASSESSMENTS

PSAs conduct voluntary, non-regulatory security surveys and assessments on critical infrastructure assets and facilities within their respective regions.

OUTREACH ACTIVITIES

PSAs conduct outreach activities with critical infrastructure owners and operators, community groups, and faith-based organizations in support of CISA priorities.

SPECIAL EVENT SUPPORT

PSAs support Federal, State, and local officials responsible for planning, leading, and coordinating NSSE and SEAR events.

INCIDENT RESPONSE

PSAs plan for and, when directed, deploy in response to natural or man-made incidents.

BOMBING PREVENTION AND AWARENESS

PSAs work in conjunction with CISA's Office for Bombing Prevention by coordinating training and materials for partners to assist in deterring, detecting, preventing, protecting against, and responding to improvised explosive device threats.v

Services

Emergency Communications Mission

CISA's Emergency Communications Division supports and promotes communications used by emergency responders and government officials to keep America safe, secure, and resilient.

HOW CISA IS CARRYING OUT ITS EMERGENCY COMMUNICATIONS MISSION:

- Expand Interoperability
- Coordinate Effective Communications Planning
- Increase Priority Services Adoption with Interoperable Priority

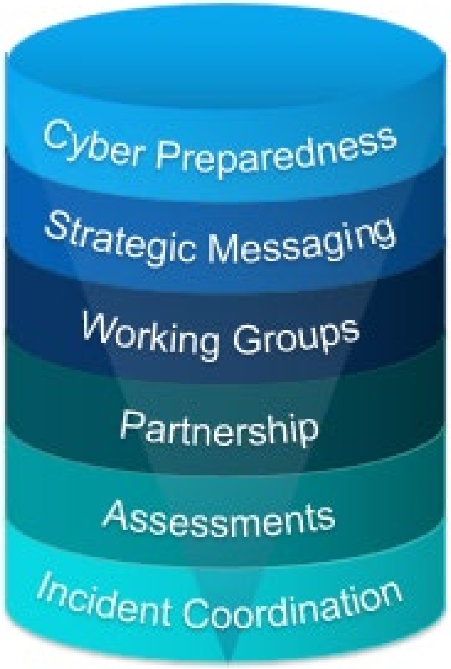
Services

Cybersecurity Advisor Program

CISA mission: Lead the collaborative national effort to strengthen the security and resilience of America’s critical infrastructure

In support of that mission: Cybersecurity Advisors (CSAs):

- **Assess**: Evaluate critical infrastructure cyber risk.
- **Promote**: Encourage best practices and risk mitigation strategies.
- **Build**: Initiate, develop capacity, and support cyber communities-of-interest and working groups.
- **Educate**: Inform and raise awareness.
- **Listen**: Collect stakeholder requirements.
- **Coordinate**: Bring together incident support and lessons learned.
- **Notifications:** Pre-ransomware notifications, vulnerability notifications, and Administrative Subpoenas



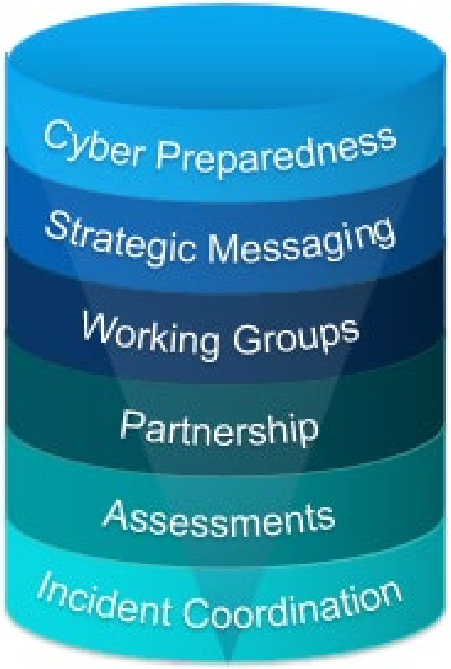
Services

Cybersecurity Advisor Program

CISA mission: Lead the collaborative national effort to strengthen the security and resilience of America's critical infrastructure

In support of that mission: Cybersecurity Advisors (CSAs):

- **Assess**: Evaluate critical infrastructure cyber risk.
- **Promote**: Encourage best practices and risk mitigation strategies.
- **Build**: Initiate, develop capacity, and support cyber communities-of-interest and working groups.
- **Educate**: Inform and raise awareness.
- **Listen**: Collect stakeholder requirements.
- **Coordinate**: Bring together incident support and lessons learned.
- **Notifications:** Pre-ransomware notifications, vulnerability notifications, and Administrative Subpoenas



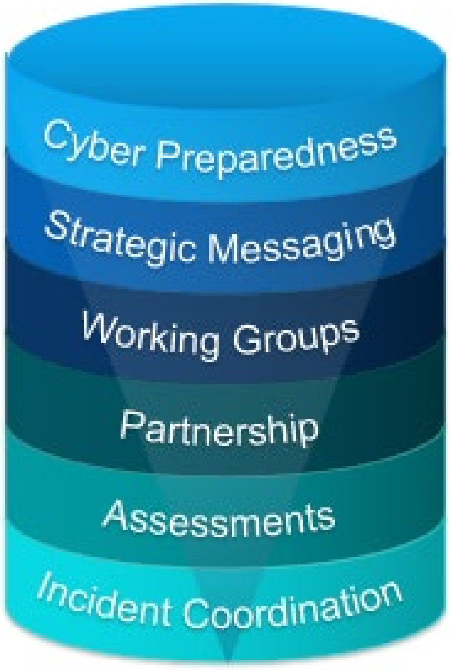
Services

Cybersecurity Advisor Program

CISA mission: Lead the collaborative national effort to strengthen the security and resilience of America's critical infrastructure

In support of that mission: Cybersecurity Advisors (CSAs):

- **Assess**: Evaluate critical infrastructure cyber risk.
- **Promote**: Encourage best practices and risk mitigation strategies.
- **Build**: Initiate, develop capacity, and support cyber communities-of-interest and working groups.
- ➡ **Educate**: Inform and raise awareness.
- **Listen**: Collect stakeholder requirements.
- **Coordinate**: Bring together incident support and lessons learned.
- **Notifications:** Pre-ransomware notifications, vulnerability notifications, and Administrative Subpoenas



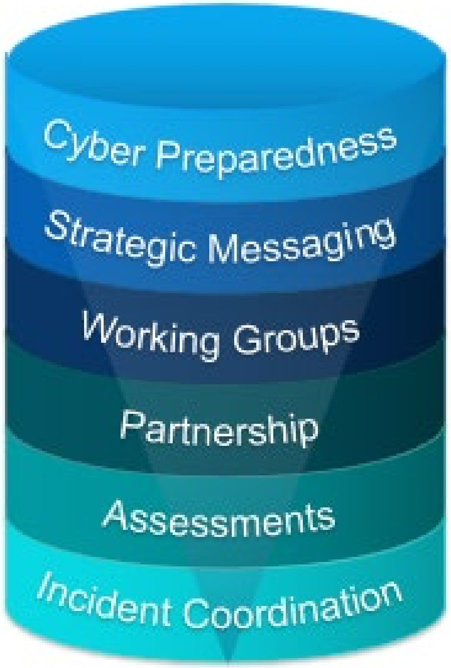
Services

Cybersecurity Advisor Program

CISA mission: Lead the collaborative national effort to strengthen the security and resilience of America’s critical infrastructure

In support of that mission: Cybersecurity Advisors (CSAs):

- **Assess**: Evaluate critical infrastructure cyber risk.
- **Promote**: Encourage best practices and risk mitigation strategies.
- **Build**: Initiate, develop capacity, and support cyber communities-of-interest and working groups.
- **Educate**: Inform and raise awareness.
- **Listen**: Collect stakeholder requirements.
- **Coordinate**: Bring together incident support and lessons learned.
- **Notifications:** Pre-ransomware notifications, vulnerability notifications, and Administrative Subpoenas



Services

Cybersecurity Services

1. Cybersecurity Advisors
2. State, Local, Tribal, and Territorial engagements
3. Cyber Education and Awareness
4. Federal Virtual Training Environment (Fed VTE)
5. National Initiative for Cybersecurity Careers and Studies
6. Stop. Think. Connect.™
7. Cybersecurity Awareness Month
8. .gov Domain
9. Request a CISA Speaker
10. Biweekly Threat Briefing
11. Information / Threat Indicator Sharing
12. Known Exploited Vulnerabilities (KEV) Catalog
13. Resource Guides
14. Cyber Incident Response Tabletop Exercise (TTX)
15. Advanced Malware Analysis Center
16. Cyber Performance Goals (CPG)
17. Ransomware Readiness Assessment (RRA)
18. Cyber Infrastructure Survey (CIS)
19. Cyber Resilience Reviews (CRR™)
20. External Dependencies Management (EDM) Assessments
21. Cyber Security Evaluation Tool (CSET™)
22. Cyber Hygiene Services

    Vulnerability Scanning

    Web Application Scanning (WAS)
23. Remote Penetration Test (RPT)
24. Risk and Vulnerability Assessment (RVA)
25. Validated Architecture Design Review (VADR)
26. Ransomware Vulnerability Warning Pilot (RVWP)
27. CyberSentry Program*
28. Secure Cloud Business Applications (SCuBA)
29. Logging Made Easy (LME)

Services

Cybersecurity Services

1. Cybersecurity Advisors
2. State, Local, Tribal, and Territorial engagements
3. Cyber Education and Awareness
4. Federal Virtual Training Environment (Fed VTE)
5. National Initiative for Cybersecurity Careers and Studies
6. Stop. Think. Connect.™
7. Cybersecurity Awareness Month
8. .gov Domain
9. Request a CISA Speaker
10. Biweekly Threat Briefing
11. Information / Threat Indicator Sharing
12. Known Exploited Vulnerabilities (KEV) Catalog
13. Resource Guides
14. Cyber Incident Response Tabletop Exercise (TTX)
15. Advanced Malware Analysis Center
16. Cyber Performance Goals (CPG)
17. Ransomware Readiness Assessment (RRA)
18. Cyber Infrastructure Survey (CIS)
19. Cyber Resilience Reviews (CRR™)
20. External Dependencies Management (EDM) Assessments
21. Cyber Security Evaluation Tool (CSET™)
22. Cyber Hygiene Services

    Vulnerability Scanning

    Web Application Scanning (WAS)
23. Remote Penetration Test (RPT)
24. Risk and Vulnerability Assessment (RVA)
25. Validated Architecture Design Review (VADR)
26. Ransomware Vulnerability Warning Pilot (RVWP)
27. CyberSentry Program*
28. Secure Cloud Business Applications (SCuBA)
29. Logging Made Easy (LME)

Services

Cybersecurity Services

1. Cybersecurity Advisors
2. State, Local, Tribal, and Territorial engagements
3. Cyber Education and Awareness
4. Federal Virtual Training Environment (Fed VTE)
5. National Initiative for Cybersecurity Careers and Studies
6. Stop. Think. Connect.™
7. Cybersecurity Awareness Month
8. .gov Domain
9. Request a CISA Speaker
10. Biweekly Threat Briefing
11. Information / Threat Indicator Sharing
12. Known Exploited Vulnerabilities (KEV) Catalog
13. Resource Guides
14. Cyber Incident Response Tabletop Exercise (TTX)
15. Advanced Malware Analysis Center
16. Cyber Performance Goals (CPG)
17. Ransomware Readiness Assessment (RRA)
18. Cyber Infrastructure Survey (CIS)
19. Cyber Resilience Reviews (CRR™)
20. External Dependencies Management (EDM) Assessments
21. Cyber Security Evaluation Tool (CSET™)
22. Cyber Hygiene Services

    Vulnerability Scanning

    Web Application Scanning (WAS)
23. Remote Penetration Test (RPT)
24. Risk and Vulnerability Assessment (RVA)
25. Validated Architecture Design Review (VADR)
26. Ransomware Vulnerability Warning Pilot (RVWP)
27. CyberSentry Program*
28. Secure Cloud Business Applications (SCuBA)
29. Logging Made Easy (LME)

Services

Cybersecurity Services

➡ 1. Cybersecurity Advisors

2. State, Local, Tribal, and Territorial engagements

➡ 3. Cyber Education and Awareness

4. Federal Virtual Training Environment (Fed VTE)
5. National Initiative for Cybersecurity Careers and Studies
6. Stop. Think. Connect.™
7. Cybersecurity Awareness Month
8. .gov Domain
9. Request a CISA Speaker
10. Biweekly Threat Briefing
11. Information / Threat Indicator Sharing
12. Known Exploited Vulnerabilities (KEV) Catalog
13. Resource Guides

➡ 14. Cyber Incident Response Tabletop Exercise (TTX)

15. Advanced Malware Analysis Center
16. Cyber Performance Goals (CPG)
17. Ransomware Readiness Assessment (RRA)
18. Cyber Infrastructure Survey (CIS)
19. Cyber Resilience Reviews (CRR™)
20. External Dependencies Management (EDM) Assessments
21. Cyber Security Evaluation Tool (CSET™)
22. Cyber Hygiene Services
    - Vulnerability Scanning
    - Web Application Scanning (WAS)
23. Remote Penetration Test (RPT)
24. Risk and Vulnerability Assessment (RVA)
25. Validated Architecture Design Review (VADR)
26. Ransomware Vulnerability Warning Pilot (RVWP)
27. CyberSentry Program*
28. Secure Cloud Business Applications (SCuBA)
29. Logging Made Easy (LME)

Services

Cybersecurity Services

➡ 1. Cybersecurity Advisors
2. State, Local, Tribal, and Territorial engagements
➡ 3. Cyber Education and Awareness
4. Federal Virtual Training Environment (Fed VTE)
5. National Initiative for Cybersecurity Careers and Studies
6. Stop. Think. Connect.™
7. Cybersecurity Awareness Month
8. .gov Domain
9. Request a CISA Speaker
10. Biweekly Threat Briefing
11. Information / Threat Indicator Sharing
12. Known Exploited Vulnerabilities (KEV) Catalog
13. Resource Guides
➡ 14. Cyber Incident Response Tabletop Exercise (TTX)
15. Advanced Malware Analysis Center

➡ 16. Cyber Performance Goals (CPG)
➡ 17. Ransomware Readiness Assessment (RRA)
18. Cyber Infrastructure Survey (CIS)
19. Cyber Resilience Reviews (CRR™)
20. External Dependencies Management (EDM) Assessments
21. Cyber Security Evaluation Tool (CSET™)
22. Cyber Hygiene Services
    Vulnerability Scanning
    Web Application Scanning (WAS)
23. Remote Penetration Test (RPT)
24. Risk and Vulnerability Assessment (RVA)
25. Validated Architecture Design Review (VADR)
26. Ransomware Vulnerability Warning Pilot (RVWP)
27. CyberSentry Program*
28. Secure Cloud Business Applications (SCuBA)
29. Logging Made Easy (LME)

Services

Cybersecurity Services

1. Cybersecurity Ad
2. State, Local, Triba
3. Cyber Education
4. Federal Virtual Tr
5. National Initiative
6. Stop. Think. Conn
7. Cybersecurity Aw
8. .gov Domain
9. Request a CISA Sp
10. Biweekly Threat
11. Information / Th
12. Known Exploited
13. Resource Guides
14. Cyber Incident R
15. Advanced Malwa

ls (CPG)
Assessment (RRA)
rvey (CIS)
vs (CRR™)
Management (EDM) Assessments
on Tool (CSET™)

ng (WAS)
st (RPT)
ssessment (RVA)
Design Review (VADR)
ity Warning Pilot (RVWP)

Applications (SCuBA)
29. Logging Made Easy (LME)

Services

Cybersecurity Services

1. ➡ Cybersecurity Advisors
2. State, Local, Tribal, and Territorial engagements
3. ➡ Cyber Education and Awareness
4. Federal Virtual Training Environment (Fed VTE)
5. National Initiative for Cybersecurity Careers and Studies
6. Stop. Think. Connect.™
7. Cybersecurity Awareness Month
8. .gov Domain
9. Request a CISA Speaker
10. Biweekly Threat Briefing
11. Information / Threat Indicator Sharing
12. Known Exploited Vulnerabilities (KEV) Catalog
13. Resource Guides
14. ➡ Cyber Incident Response Tabletop Exercise (TTX)
15. Advanced Malware Analysis Center
16. ➡ Cyber Performance Goals (CPG)
17. ➡ Ransomware Readiness Assessment (RRA)
18. Cyber Infrastructure Survey (CIS)
19. Cyber Resilience Reviews (CRR™)
20. External Dependencies Management (EDM) Assessments
21. Cyber Security Evaluation Tool (CSET™)
22. ➡ Cyber Hygiene Services
    Vulnerability Scanning
    Web Application Scanning (WAS)
23. Remote Penetration Test (RPT)
24. Risk and Vulnerability Assessment (RVA)
25. Validated Architecture Design Review (VADR)
26. Ransomware Vulnerability Warning Pilot (RVWP)
27. CyberSentry Program*
28. Secure Cloud Business Applications (SCuBA)
29. Logging Made Easy (LME)

Services

Cybersecurity Services

1. Cybersecurity Advisors
2. State, Local, Tribal, and Territorial engagements
3. Cyber Education and Awareness
4. Federal Virtual Training Environment (Fed VTE)
5. National Initiative for Cybersecurity Careers and Studies
6. Stop. Think. Connect.™
7. Cybersecurity Awareness Month
8. .gov Domain
9. Request a CISA Speaker
10. Biweekly Threat Briefing
11. Information / Threat Indicator Sharing
12. Known Exploited Vulnerabilities (KEV) Catalog
13. Resource Guides
14. Cyber Incident Response Tabletop Exercise (TTX)
15. Advanced Malware Analysis Center
16. Cyber Performance Goals (CPG)
17. Ransomware Readiness Assessment (RRA)
18. Cyber Infrastructure Survey (CIS)
19. Cyber Resilience Reviews (CRR™)
20. External Dependencies Management (EDM) Assessments
21. Cyber Security Evaluation Tool (CSET™)
22. Cyber Hygiene Services

    Vulnerability Scanning

    Web Application Scanning (WAS)
23. Remote Penetration Test (RPT)
24. Risk and Vulnerability Assessment (RVA)
25. Validated Architecture Design Review (VADR)
26. Ransomware Vulnerability Warning Pilot (RVWP)
27. CyberSentry Program*
28. Secure Cloud Business Applications (SCuBA)
29. Logging Made Easy (LME)

Services

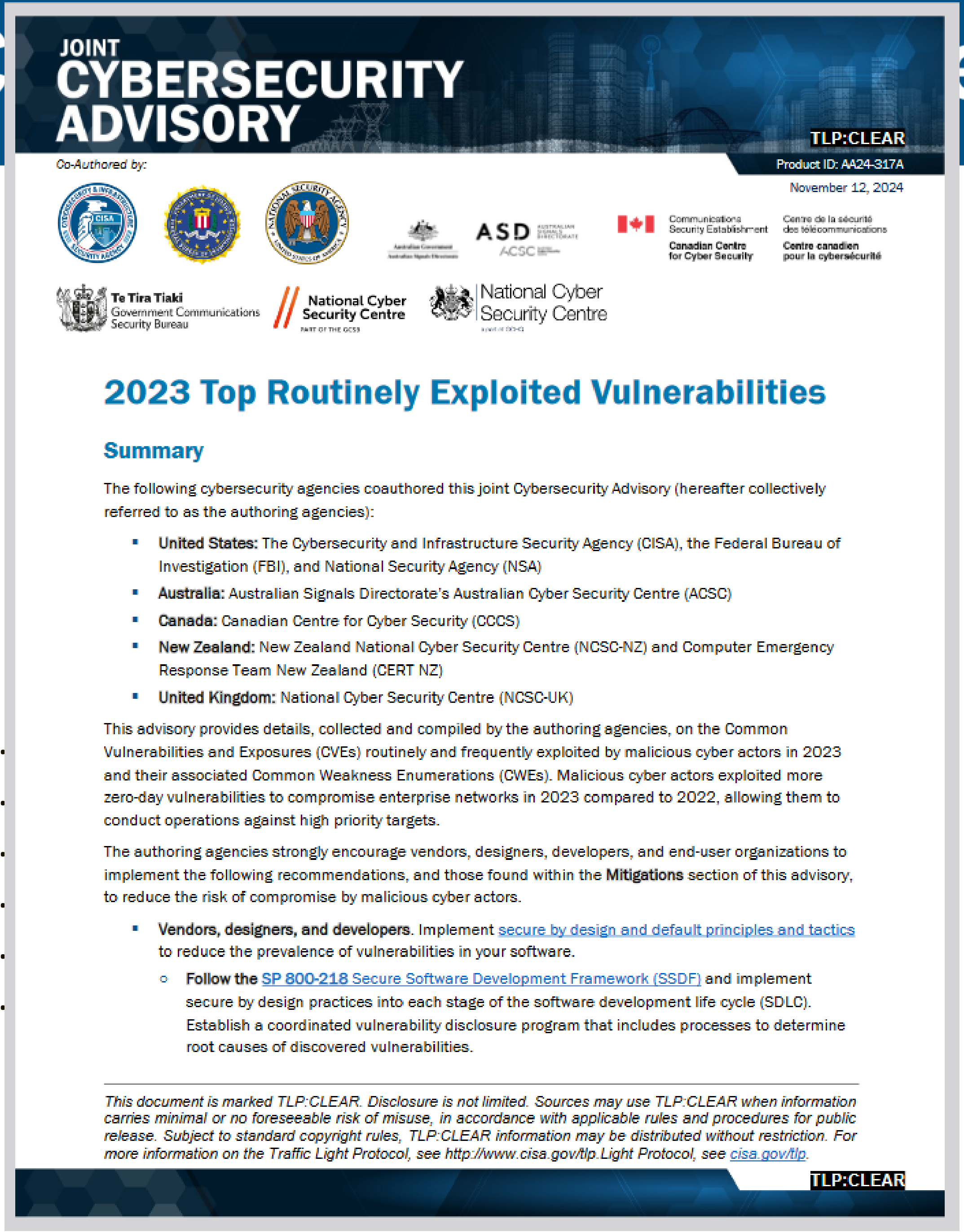
Cybersecurity Services

➡ 1. Cybersecurity Advisors
2. State, Local, Tribal, and Territorial engagements
➡ 3. Cyber Education and Awareness
4. Federal Virtual Training Environment (Fed VTE)
5. National Initiative for Cybersecurity Careers and Studies
6. Stop. Think. Connect.™
7. Cybersecurity Awareness Month
8. .gov Domain
9. Request a CISA Speaker
10. Biweekly Threat Briefing
11. Information / Threat Indicator Sharing
12. Known Exploited Vulnerabilities (KEV) Catalog
13. Resource Guides
➡ 14. Cyber Incident Response Tabletop Exercise (TTX)
15. Advanced Malware Analysis Center

➡ 16. Cyber Performance Goals (CPG)
➡ 17. Ransomware Readiness Assessment (RRA)
18. Cyber Infrastructure Survey (CIS)
19. Cyber Resilience Reviews (CRR™)
20. External Dependencies Management (EDM) Assessments
21. Cyber Security Evaluation Tool (CSET™)
➡ 22. Cyber Hygiene Services
Vulnerability Scanning
Web Application Scanning (WAS)
23. Remote Penetration Test (RPT)
24. Risk and Vulnerability Assessment (RVA)
25. Validated Architecture Design Review (VADR)
26. Ransomware Vulnerability Warning Pilot (RVWP)
27. CyberSentry Program*
➡ 28. Secure Cloud Business Applications (SCuBA)
➡ 29. Logging Made Easy (LME)

Services

C es



JOINT
CYBERSECURITY
ADVISORY

TLP:CLEAR

Product ID: AA24-317A

November 12, 2024

Co-Authored by:

ASD
ACSC

Communications Security Establishment
Canadian Centre for Cyber Security

Centre de la sécurité des télécommunications
Centre canadien pour la cybersécurité

Te Tira Tiaki
Government Communications Security Bureau

National Cyber Security Centre

National Cyber Security Centre

2023 Top Routinely Exploited Vulnerabilities

Summary

The following cybersecurity agencies coauthored this joint Cybersecurity Advisory (hereafter collectively referred to as the authoring agencies):

- **United States:** The Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and National Security Agency (NSA)
- **Australia:** Australian Signals Directorate's Australian Cyber Security Centre (ACSC)
- **Canada:** Canadian Centre for Cyber Security (CCCS)
- **New Zealand:** New Zealand National Cyber Security Centre (NCSC-NZ) and Computer Emergency Response Team New Zealand (CERT NZ)
- **United Kingdom:** National Cyber Security Centre (NCSC-UK)

This advisory provides details, collected and compiled by the authoring agencies, on the Common Vulnerabilities and Exposures (CVEs) routinely and frequently exploited by malicious cyber actors in 2023 and their associated Common Weakness Enumerations (CWEs). Malicious cyber actors exploited more zero-day vulnerabilities to compromise enterprise networks in 2023 compared to 2022, allowing them to conduct operations against high priority targets.

The authoring agencies strongly encourage vendors, designers, developers, and end-user organizations to implement the following recommendations, and those found within the **Mitigations** section of this advisory, to reduce the risk of compromise by malicious cyber actors.

- **Vendors, designers, and developers.** Implement secure by design and default principles and tactics to reduce the prevalence of vulnerabilities in your software.
    - **Follow the** SP 800-218 Secure Software Development Framework (SSDF) and implement secure by design practices into each stage of the software development life cycle (SDLC). Establish a coordinated vulnerability disclosure program that includes processes to determine root causes of discovered vulnerabilities.

This document is marked TLP:CLEAR. Disclosure is not limited. Sources may use TLP:CLEAR 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:CLEAR information may be distributed without restriction. For more information on the Traffic Light Protocol, see http://www.cisa.gov/tlp.Light Protocol, see cisa.gov/tlp.

TLP:CLEAR

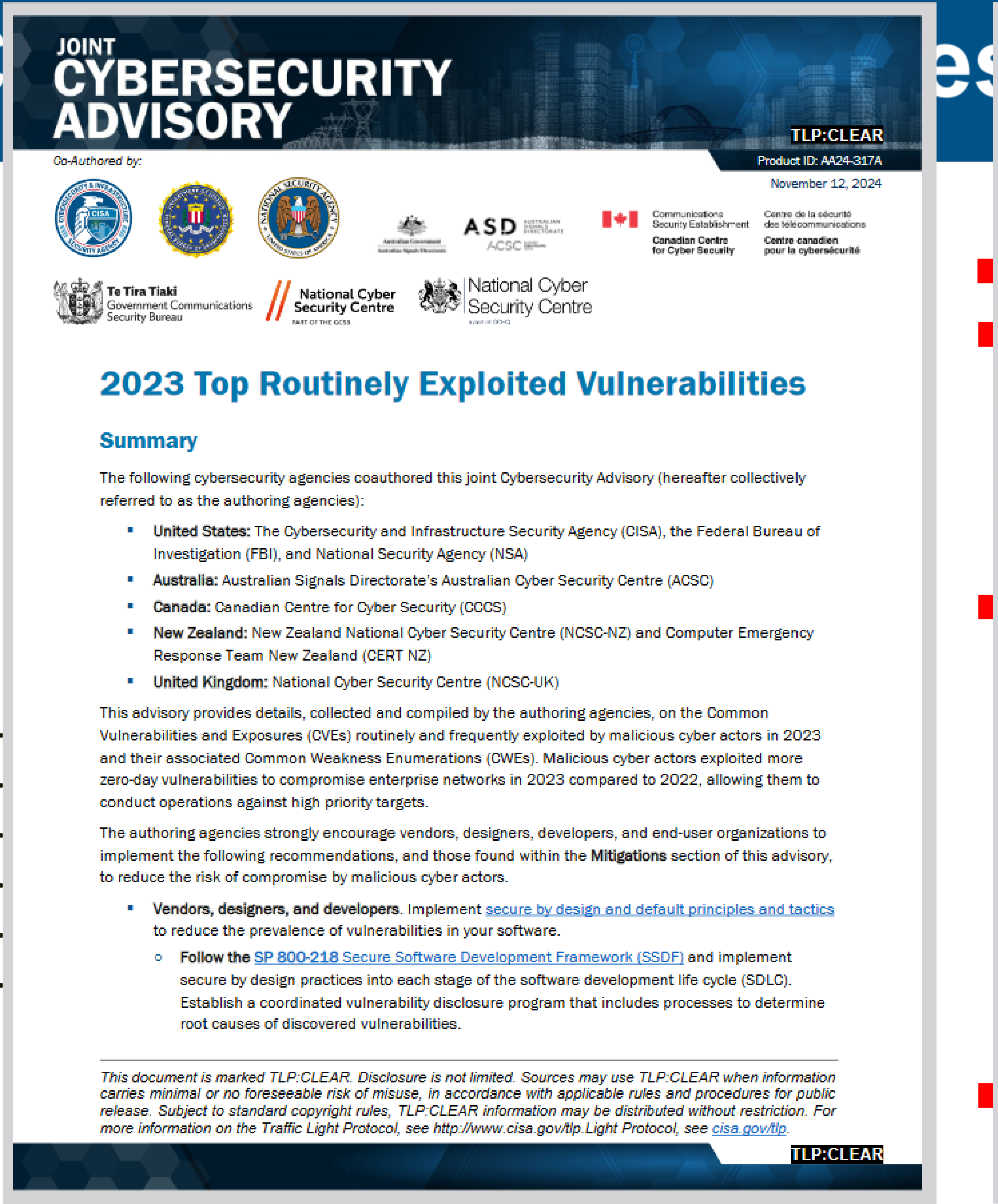
1.
2.
3.
4.
5.
6.
7.
8.
9.
10.
11.
12.
13.
14.
15.

16. Cyber Performance Goals (CPG)
17. Ransomware Readiness Assessment (RRA)
18. Cyber Infrastructure Survey (CIS)
19. Cyber Resilience Reviews (CRR™)
20. External Dependencies Management (EDM) Assessments
21. Cyber Security Evaluation Tool (CSET™)
22. Cyber Hygiene Services
    Vulnerability Scanning
    Web Application Scanning (WAS)
23. Remote Penetration Test (RPT)
24. Risk and Vulnerability Assessment (RVA)
25. Validated Architecture Design Review (VADR)
26. Ransomware Vulnerability Warning Pilot (RVWP)
27. CyberSentry Program*
28. Secure Cloud Business Applications (SCuBA)
29. Logging Made Easy (LME)

Services

C es

1.
2.
3.
4.
5.
6.
7.
8.
9.
10.
11.
12.
13.
14.
15.



JOINT CYBERSECURITY ADVISORY

TLP:CLEAR

Co-Authored by:

Product ID: AA24-317A

November 12, 2024

2023 Top Routinely Exploited Vulnerabilities

Summary

The following cybersecurity agencies coauthored this joint Cybersecurity Advisory (hereafter collectively referred to as the authoring agencies):

- **United States:** The Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and National Security Agency (NSA)
- **Australia:** Australian Signals Directorate's Australian Cyber Security Centre (ACSC)
- **Canada:** Canadian Centre for Cyber Security (CCCS)
- **New Zealand:** New Zealand National Cyber Security Centre (NCSC-NZ) and Computer Emergency Response Team New Zealand (CERT NZ)
- **United Kingdom:** National Cyber Security Centre (NCSC-UK)

This advisory provides details, collected and compiled by the authoring agencies, on the Common Vulnerabilities and Exposures (CVEs) routinely and frequently exploited by malicious cyber actors in 2023 and their associated Common Weakness Enumerations (CWEs). Malicious cyber actors exploited more zero-day vulnerabilities to compromise enterprise networks in 2023 compared to 2022, allowing them to conduct operations against high priority targets.

The authoring agencies strongly encourage vendors, designers, developers, and end-user organizations to implement the following recommendations, and those found within the **Mitigations** section of this advisory, to reduce the risk of compromise by malicious cyber actors.

- **Vendors, designers, and developers**. Implement secure by design and default principles and tactics to reduce the prevalence of vulnerabilities in your software.
  - **Follow the** SP 800-218 Secure Software Development Framework (SSDF) and implement secure by design practices into each stage of the software development life cycle (SDLC). Establish a coordinated vulnerability disclosure program that includes processes to determine root causes of discovered vulnerabilities.

This document is marked TLP:CLEAR. Disclosure is not limited. Sources may use TLP:CLEAR 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:CLEAR information may be distributed without restriction. For more information on the Traffic Light Protocol, see http://www.cisa.gov/tlp.Light Protocol, see cisa.gov/tlp.

TLP:CLEAR

TLP:CLEAR

JOINT CYBER DEFENSE COLLABORATIVE

SECURE BY DESIGN

Safe Software Deployment: How Software Manufacturers Can Ensure Reliability for Customers

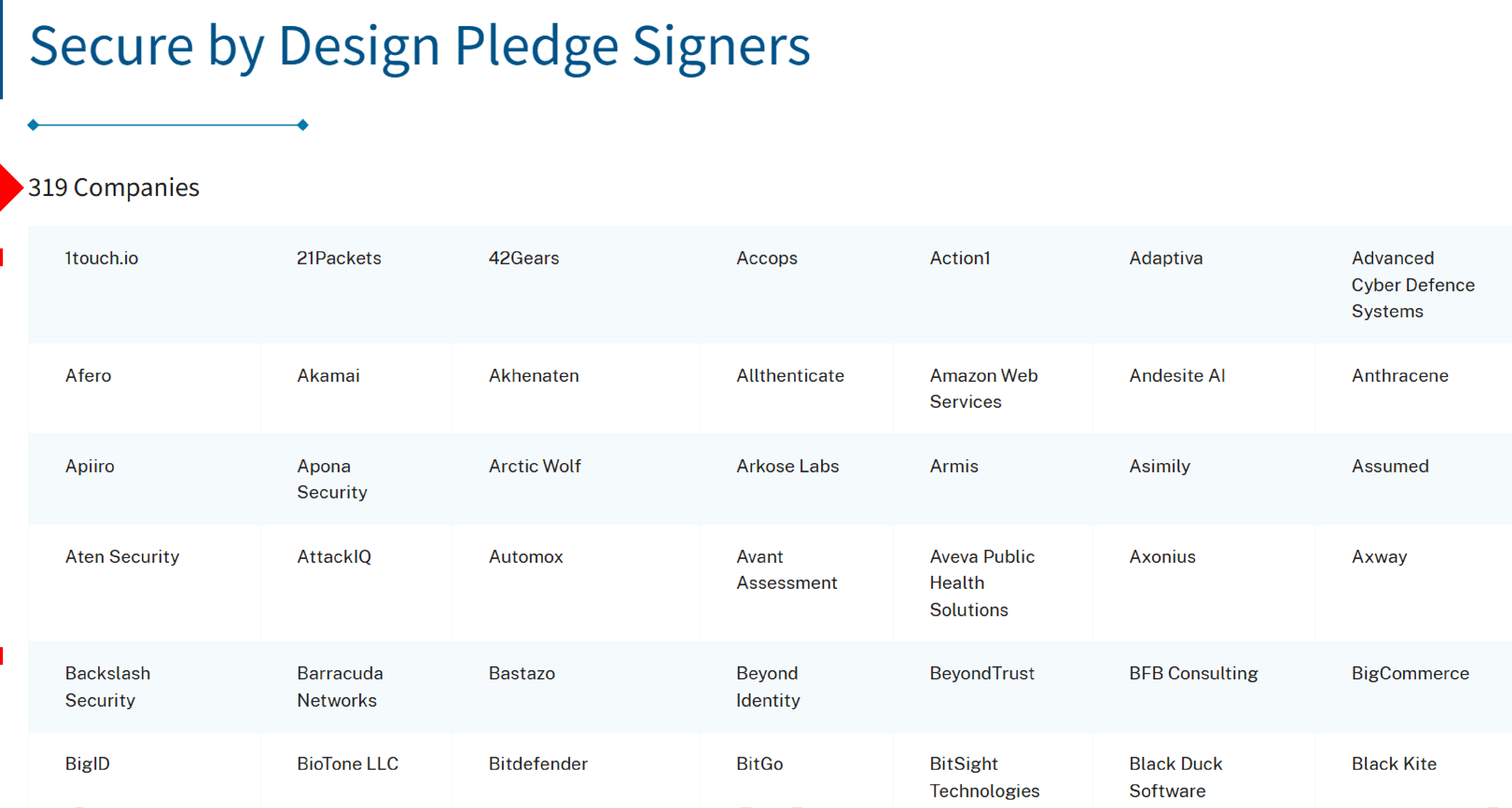
Publication: October 2024

Cybersecurity and Infrastructure Security Agency
Federal Bureau of Investigation
Australian Signals Directorate's Australian Cyber Security Centre

This document is distributed as TLP:CLEAR. Recipients may distribute TLP:CLEAR information without restrictions. Information is subject to standard copyright rules. For more information on the Traffic Light Protocol, see cisa.gov/tlp.

TLP:CLEAR

nents



Secure by Design Pledge Signers

319 Companies

1touch.io	21Packets	42Gears	Accops	Action1	Adaptiva	Advanced Cyber Defence Systems
Afero	Akamai	Akhenaten	Allthenticate	Amazon Web Services	Andesite AI	Anthracene
Apiiro	Apona Security	Arctic Wolf	Arkose Labs	Armis	Asimily	Assumed
Aten Security	AttackIQ	Automox	Avant Assessment	Aveva Public Health Solutions	Axonius	Axway
Backslash Security	Barracuda Networks	Bastazo	Beyond Identity	BeyondTrust	BFB Consulting	BigCommerce
BigID	BioTone LLC	Bitdefender	BitGo	BitSight Technologies	Black Duck Software	Black Kite

ents

TLP:CLEAR

Cybersecurity Services

➡ 1. Cybersecurity Advisors

2. State, Local, Tribal, and Territorial engagements

➡ 3. Cyber Education and Awareness

4. Federal Virtual Training Environment (Fed VTE)

5. National Initiative for Cybersecurity Careers and Studies

6. Stop. Think. Connect.™

7. Cybersecurity Awareness Month

8. .gov Domain

9. Request a CISA Speaker

10. Biweekly Threat Briefing

11. Information / Threat Indicator Sharing

12. Known Exploited Vulnerabilities (KEV) Catalog

13. Resource Guides

➡ 14. Cyber Incident Response Tabletop Exercise (TTX)

15. Advanced Malware Analysis Center

➡ 16. Cyber Performance Goals (CPG)

➡ 17. Ransomware Readiness Assessment (RRA)

18. Cyber Infrastructure Survey (CIS)

19. Cyber Resilience Reviews (CRR™)

20. External Dependencies Management (EDM) Assessments

21. Cyber Security Evaluation Tool (CSET™)

➡ 22. Cyber Hygiene Services

Vulnerability Scanning

Web Application Scanning (WAS)

23. Remote Penetration Test (RPT)

24. Risk and Vulnerability Assessment (RVA)

25. Validated Architecture Design Review (VADR)

26. Ransomware Vulnerability Warning Pilot (RVWP)

27. CyberSentry Program*

➡ 28. Secure Cloud Business Applications (SCuBA)

➡ 29. Logging Made Easy (LME)

ZERO COST

Services

Cybersecurity Advisor Program

Left of

CYBER
ATTACKS

Services

Cybersecurity Advisor Program

Left of

CYBER
ATTACKS

Cybersecurity Advisor Program

Left of

Notifications

Cybersecurity Advisor Program

Left of

Notifications

Cybersecurity Advisor Program

Left of

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
CISA
CALIFORNIA CYBER SECURITY INTEGRATION CENTER
STATE OF CALIFORNIA
INDICIUM • INTEGRATIONEM • AUCTORITAS
CAL - CSIC
DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
FIDELITY BRAVERY INTEGRITY
UNITED STATES SECRET SERVICE
HOMELAND SECURITY INVESTIGATIONS
HSI
U S
SPECIAL AGENT
U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT

Notifications

Cybersecurity Advisor Program

Left of

Right of

Notifications

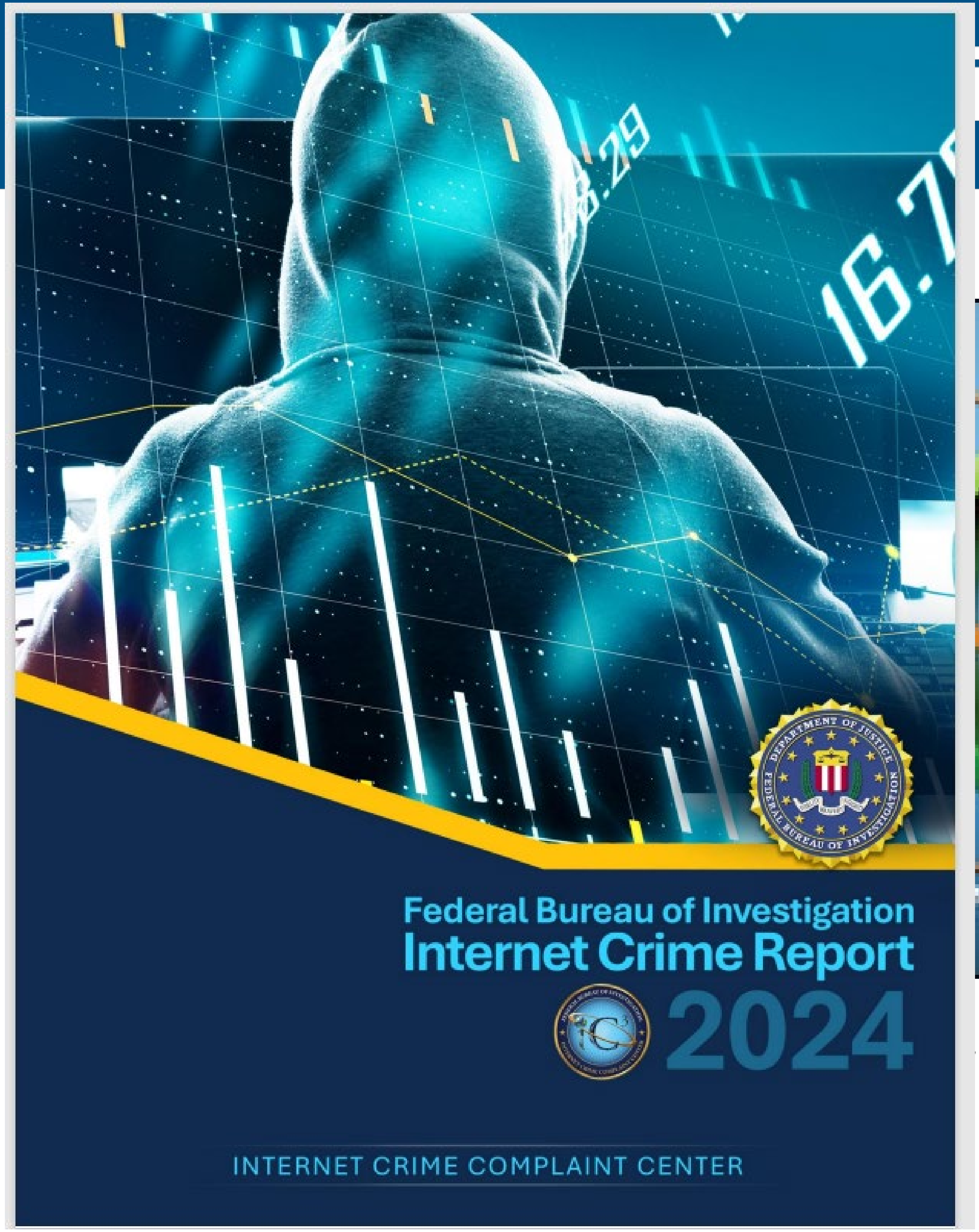
Cybersecurity Advisor Program

Left o

Right of

www.IC3.gov

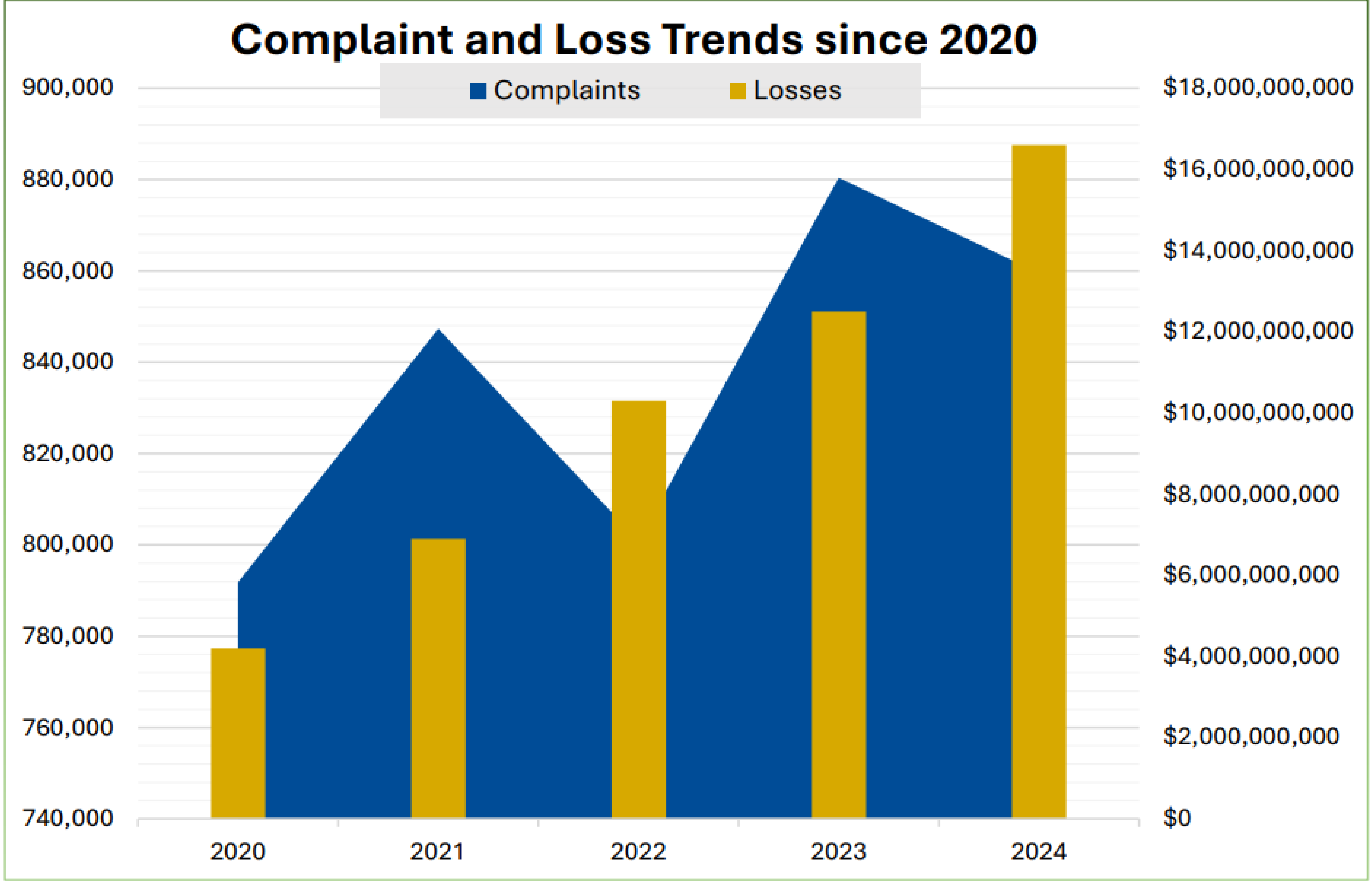
isor Program

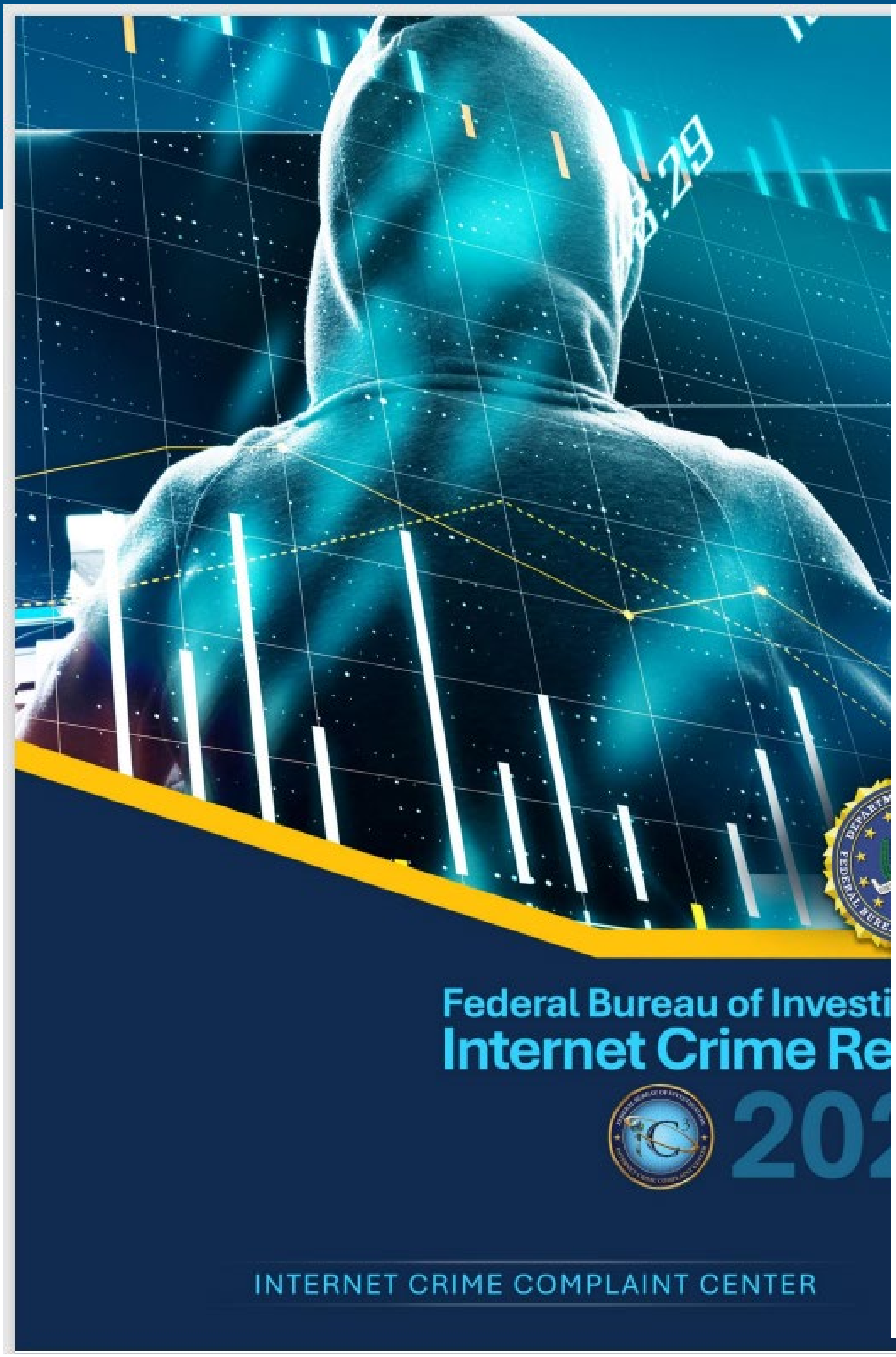


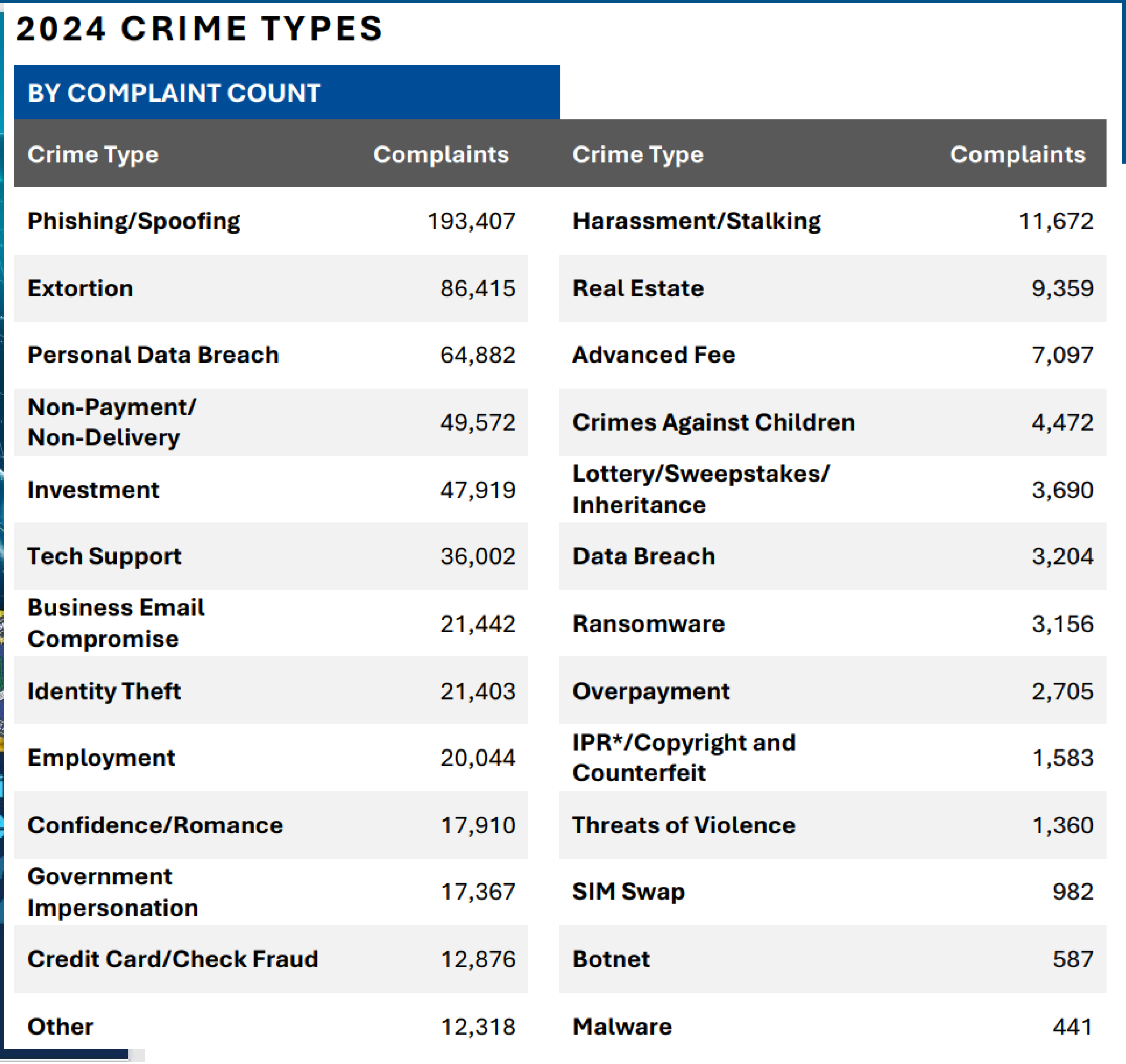
Federal Bureau of Investigation
Internet Crime Report
2024

INTERNET CRIME COMPLAINT CENTER

w.IC3.gov


Complaint and Loss Trends since 2020

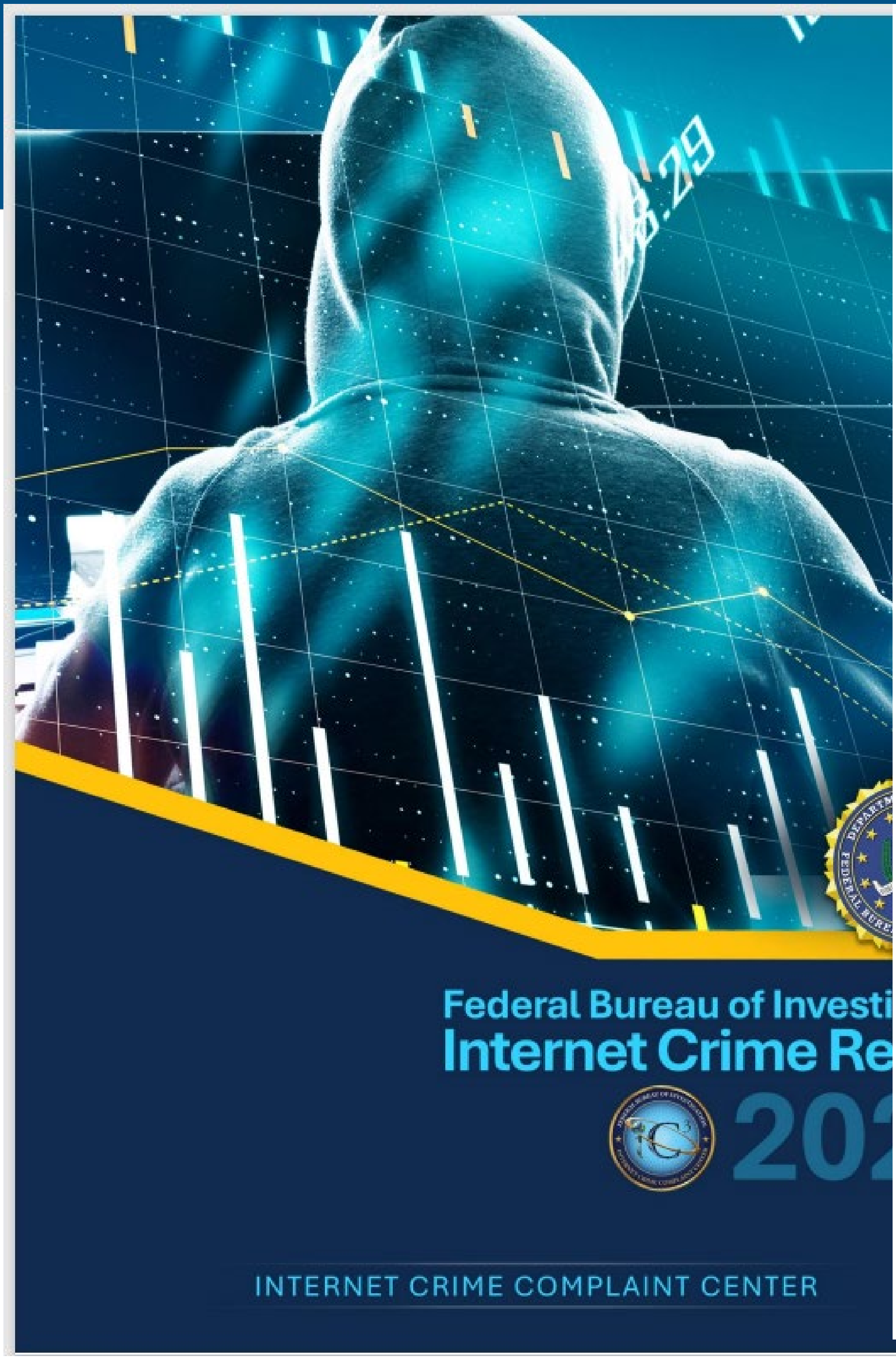


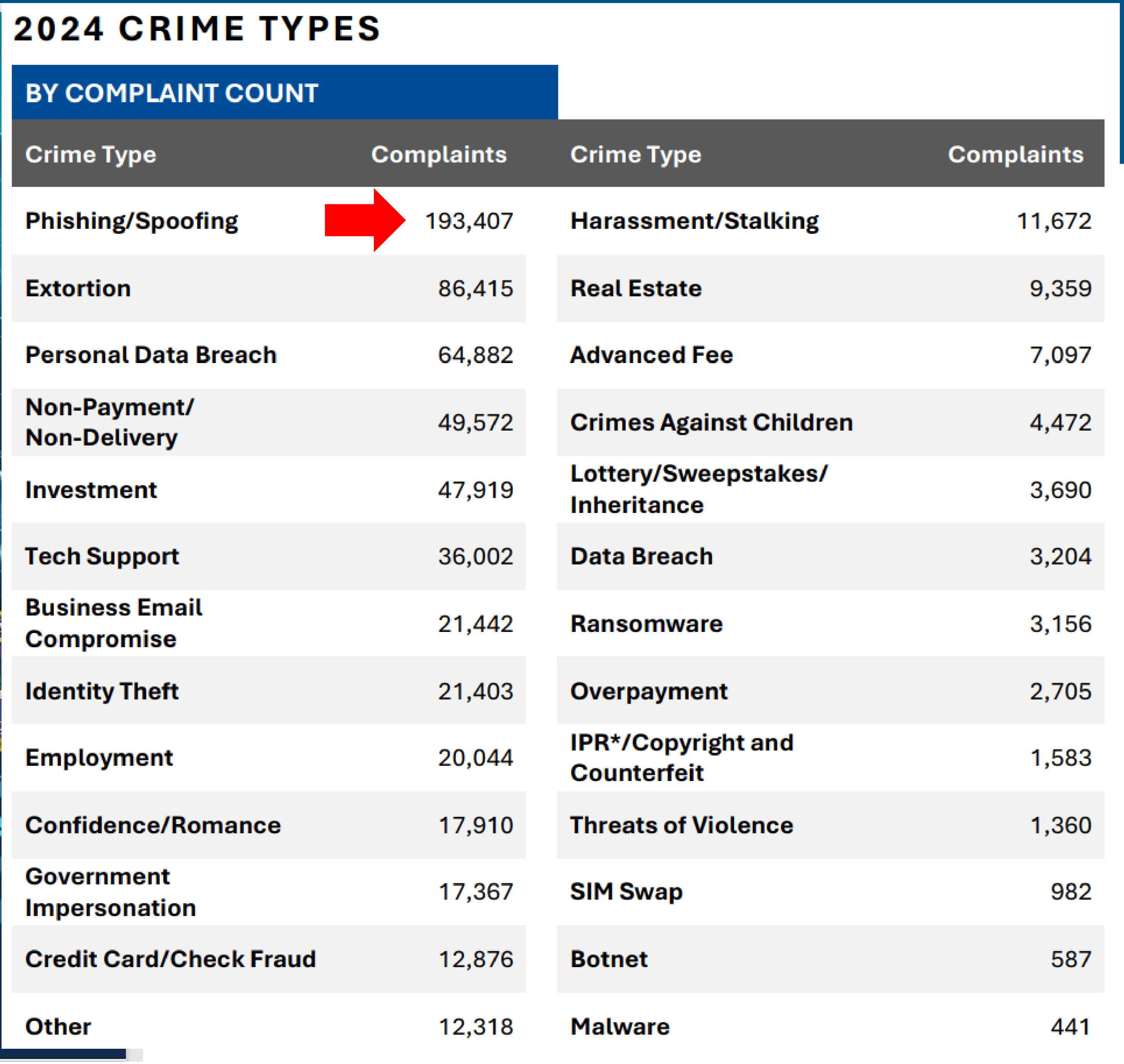


2024 CRIME TYPES

BY COMPLAINT COUNT

Crime Type	Complaints	Crime Type	Complaints
Phishing/Spoofing	193,407	Harassment/Stalking	11,672
Extortion	86,415	Real Estate	9,359
Personal Data Breach	64,882	Advanced Fee	7,097
Non-Payment/ Non-Delivery	49,572	Crimes Against Children	4,472
Investment	47,919	Lottery/Sweepstakes/ Inheritance	3,690
Tech Support	36,002	Data Breach	3,204
Business Email Compromise	21,442	Ransomware	3,156
Identity Theft	21,403	Overpayment	2,705
Employment	20,044	IPR*/Copyright and Counterfeit	1,583
Confidence/Romance	17,910	Threats of Violence	1,360
Government Impersonation	17,367	SIM Swap	982
Credit Card/Check Fraud	12,876	Botnet	587
Other	12,318	Malware	441

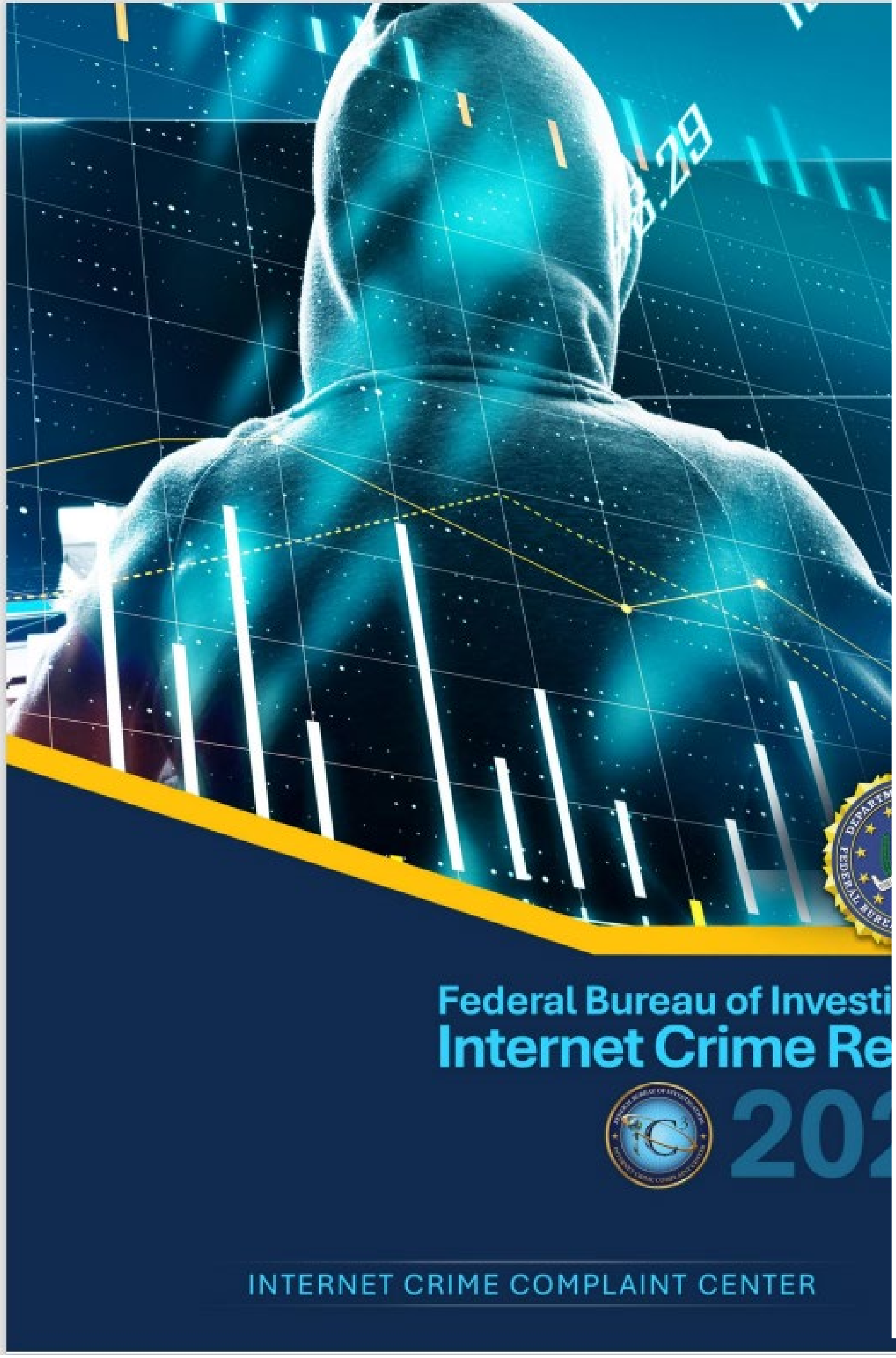


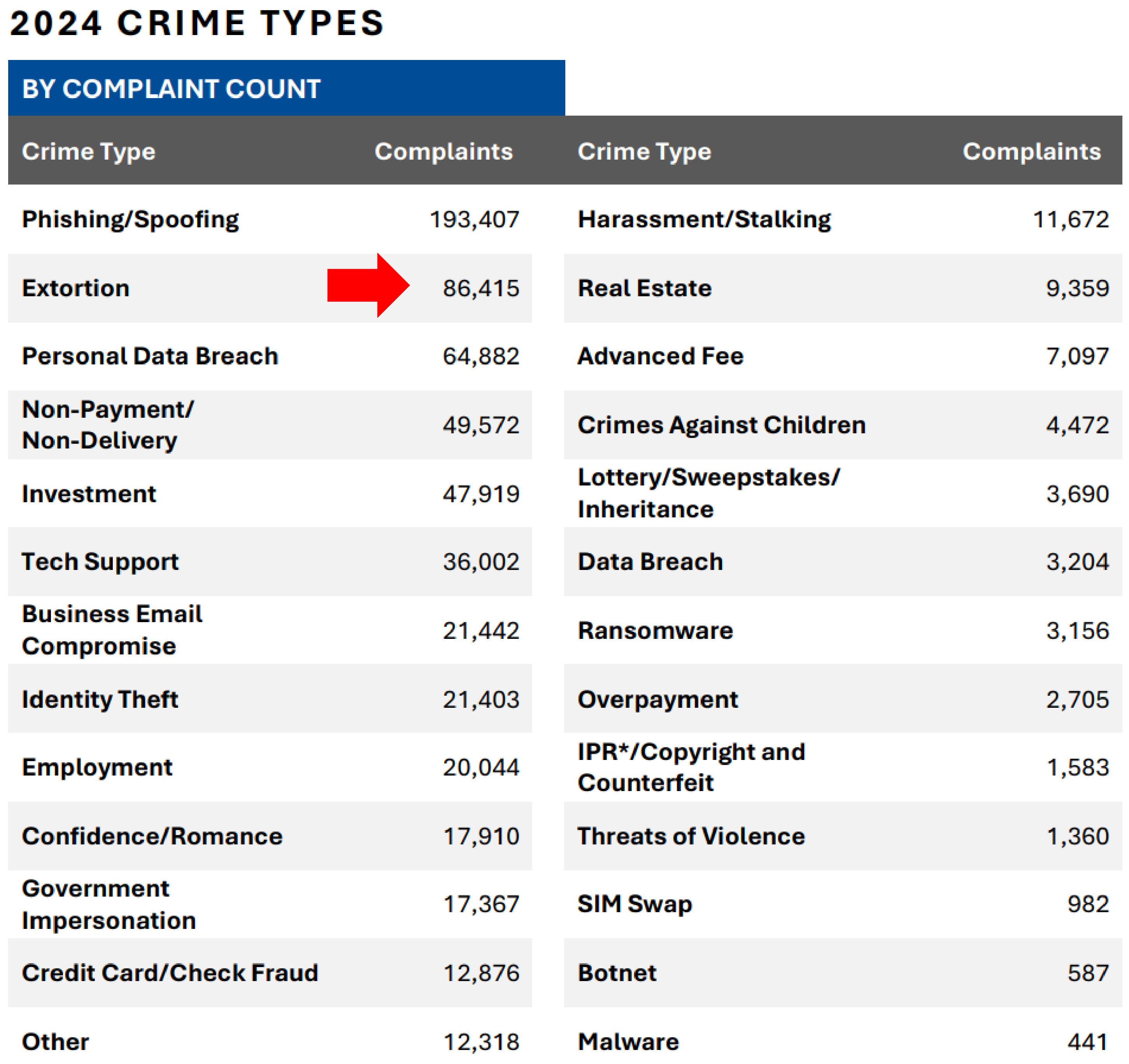


2024 CRIME TYPES

BY COMPLAINT COUNT

Crime Type	Complaints	Crime Type	Complaints
Phishing/Spoofing	193,407	Harassment/Stalking	11,672
Extortion	86,415	Real Estate	9,359
Personal Data Breach	64,882	Advanced Fee	7,097
Non-Payment/ Non-Delivery	49,572	Crimes Against Children	4,472
Investment	47,919	Lottery/Sweepstakes/ Inheritance	3,690
Tech Support	36,002	Data Breach	3,204
Business Email Compromise	21,442	Ransomware	3,156
Identity Theft	21,403	Overpayment	2,705
Employment	20,044	IPR*/Copyright and Counterfeit	1,583
Confidence/Romance	17,910	Threats of Violence	1,360
Government Impersonation	17,367	SIM Swap	982
Credit Card/Check Fraud	12,876	Botnet	587
Other	12,318	Malware	441

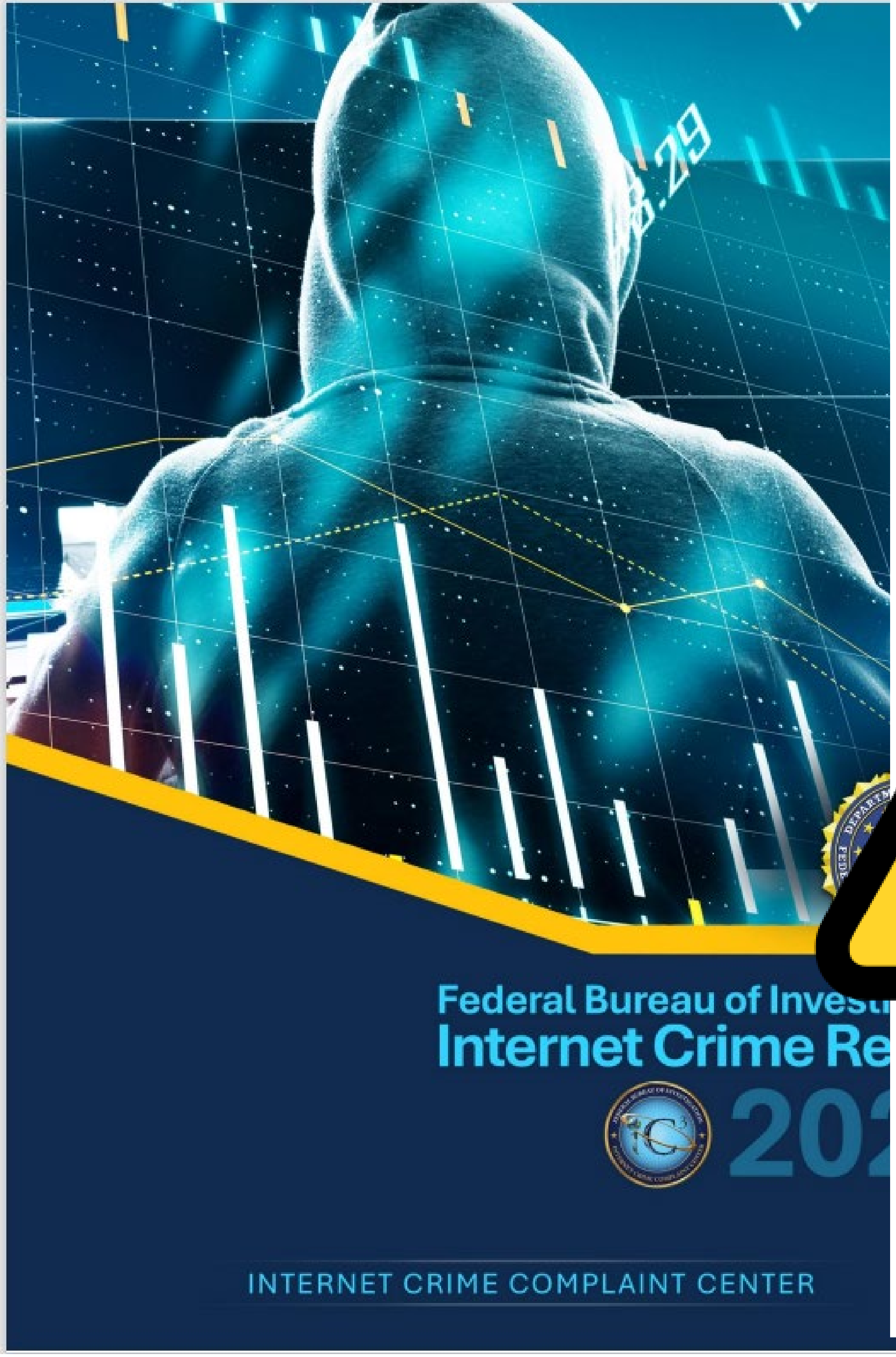


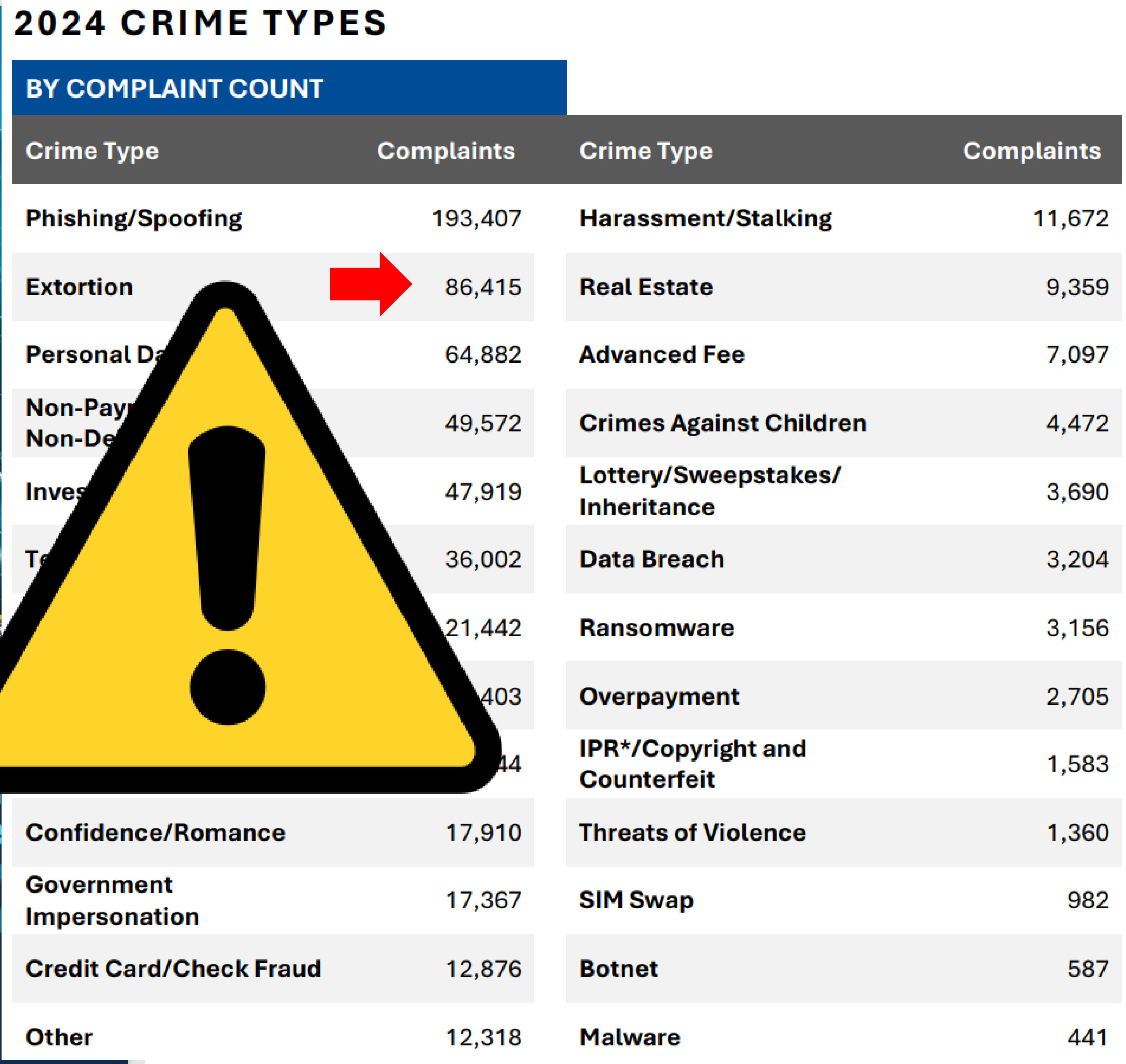


2024 CRIME TYPES

BY COMPLAINT COUNT

Crime Type	Complaints	Crime Type	Complaints
Phishing/Spoofing	193,407	Harassment/Stalking	11,672
Extortion	86,415	Real Estate	9,359
Personal Data Breach	64,882	Advanced Fee	7,097
Non-Payment/ Non-Delivery	49,572	Crimes Against Children	4,472
Investment	47,919	Lottery/Sweepstakes/ Inheritance	3,690
Tech Support	36,002	Data Breach	3,204
Business Email Compromise	21,442	Ransomware	3,156
Identity Theft	21,403	Overpayment	2,705
Employment	20,044	IPR*/Copyright and Counterfeit	1,583
Confidence/Romance	17,910	Threats of Violence	1,360
Government Impersonation	17,367	SIM Swap	982
Credit Card/Check Fraud	12,876	Botnet	587
Other	12,318	Malware	441

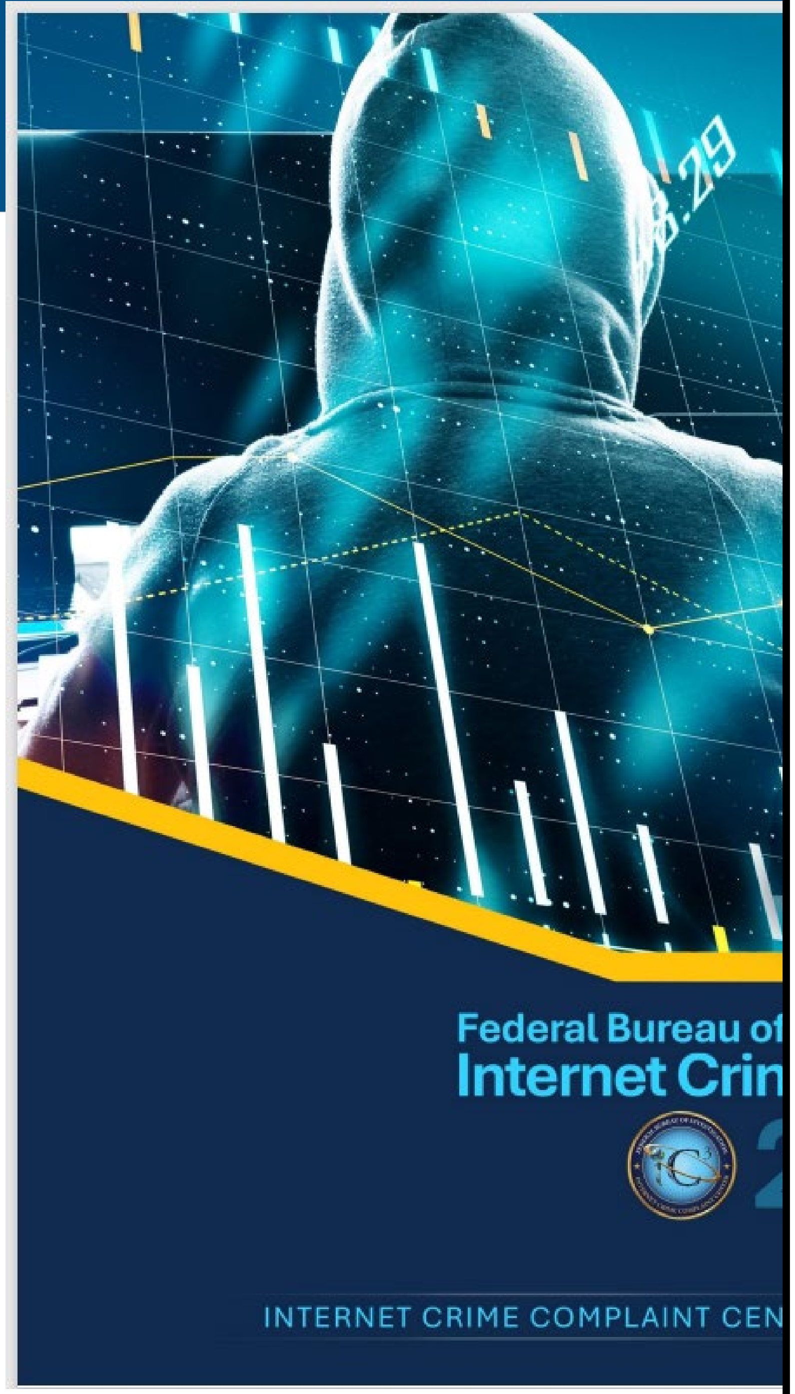


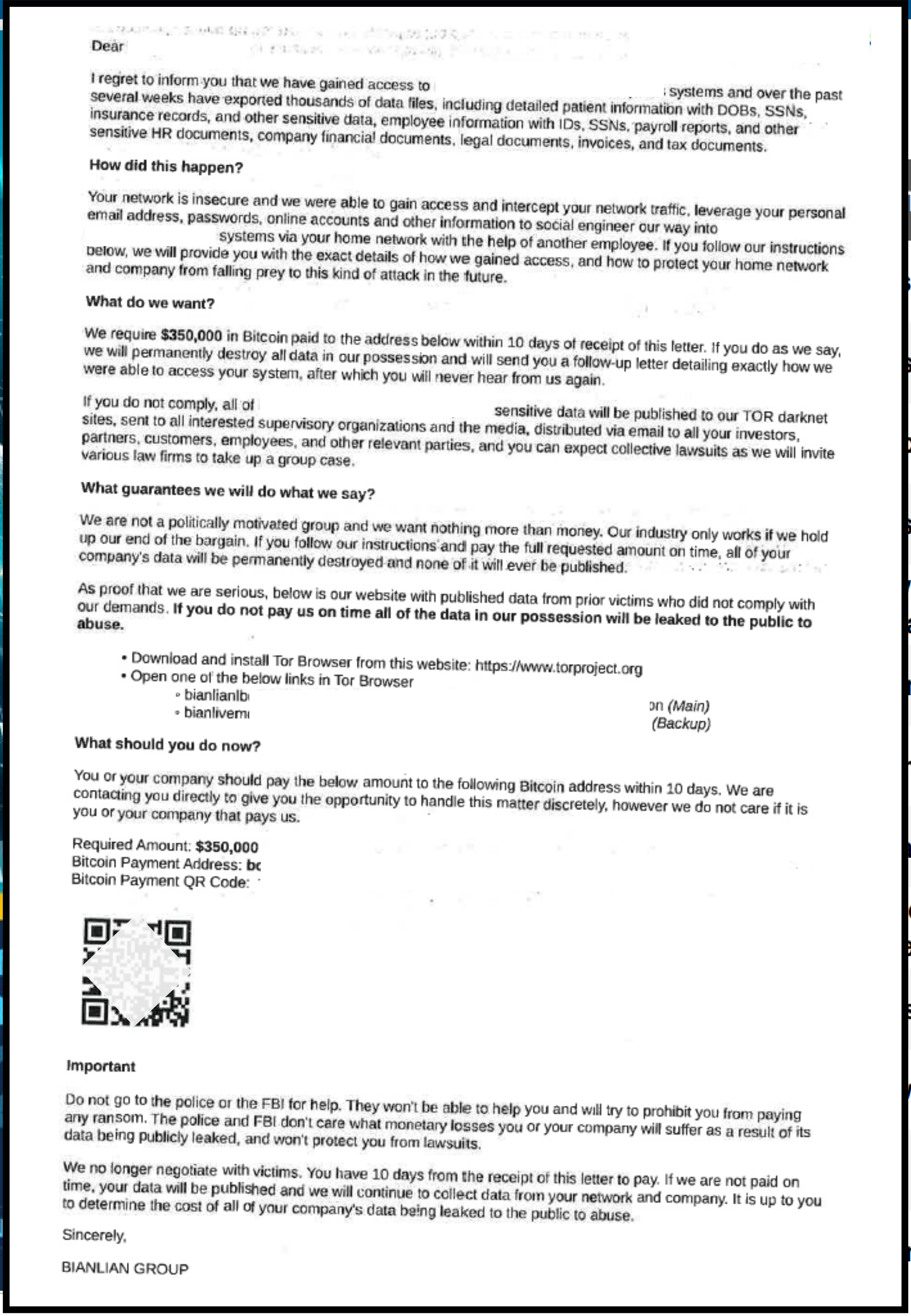


2024 CRIME TYPES

BY COMPLAINT COUNT

Crime Type	Complaints	Crime Type	Complaints
Phishing/Spoofing	193,407	Harassment/Stalking	11,672
Extortion	86,415	Real Estate	9,359
Personal Da	64,882	Advanced Fee	7,097
Non-Pay Non-De	49,572	Crimes Against Children	4,472
Inves	47,919	Lottery/Sweepstakes/ Inheritance	3,690
Te	36,002	Data Breach	3,204
[illegible]	21,442	Ransomware	3,156
[illegible]	403	Overpayment	2,705
[illegible]	44	IPR*/Copyright and Counterfeit	1,583
Confidence/Romance	17,910	Threats of Violence	1,360
Government Impersonation	17,367	SIM Swap	982
Credit Card/Check Fraud	12,876	Botnet	587
Other	12,318	Malware	441





Dear

I regret to inform you that we have gained access to systems and over the past several weeks have exported thousands of data files, including detailed patient information with DOBs, SSNs, insurance records, and other sensitive data, employee information with IDs, SSNs, payroll reports, and other sensitive HR documents, company financial documents, legal documents, invoices, and tax documents.

How did this happen?

Your network is insecure and we were able to gain access and intercept your network traffic, leverage your personal email address, passwords, online accounts and other information to social engineer our way into systems via your home network with the help of another employee. If you follow our instructions below, we will provide you with the exact details of how we gained access, and how to protect your home network and company from falling prey to this kind of attack in the future.

What do we want?

We require **$350,000** in Bitcoin paid to the address below within 10 days of receipt of this letter. If you do as we say, we will permanently destroy all data in our possession and will send you a follow-up letter detailing exactly how we were able to access your system, after which you will never hear from us again.

If you do not comply, all of sensitive data will be published to our TOR darknet sites, sent to all interested supervisory organizations and the media, distributed via email to all your investors, partners, customers, employees, and other relevant parties, and you can expect collective lawsuits as we will invite various law firms to take up a group case.

What guarantees we will do what we say?

We are not a politically motivated group and we want nothing more than money. Our industry only works if we hold up our end of the bargain. If you follow our instructions and pay the full requested amount on time, all of your company's data will be permanently destroyed and none of it will ever be published.

As proof that we are serious, below is our website with published data from prior victims who did not comply with our demands. **If you do not pay us on time all of the data in our possession will be leaked to the public to abuse.**

- Download and install Tor Browser from this website: https://www.torproject.org
- Open one of the below links in Tor Browser
  - bianlianlb on *(Main)*
  - bianlivem *(Backup)*

What should you do now?

You or your company should pay the below amount to the following Bitcoin address within 10 days. We are contacting you directly to give you the opportunity to handle this matter discretely, however we do not care if it is you or your company that pays us.

Required Amount: **$350,000**
Bitcoin Payment Address: **bc**
Bitcoin Payment QR Code:

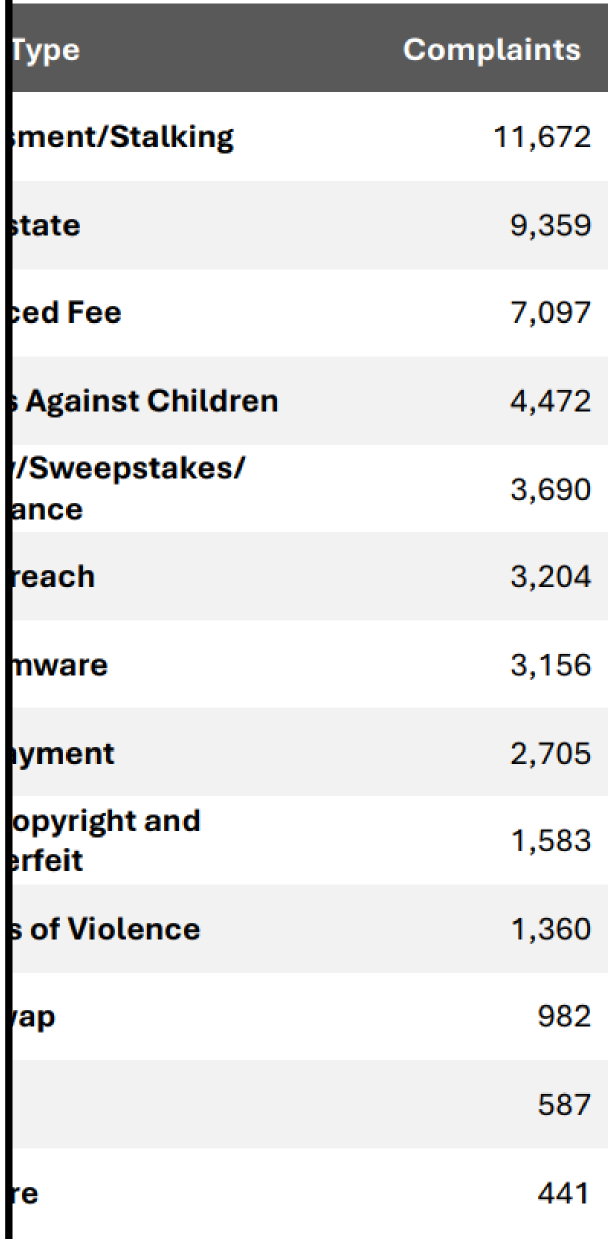
Important

Do not go to the police or the FBI for help. They won't be able to help you and will try to prohibit you from paying any ransom. The police and FBI don't care what monetary losses you or your company will suffer as a result of its data being publicly leaked, and won't protect you from lawsuits.

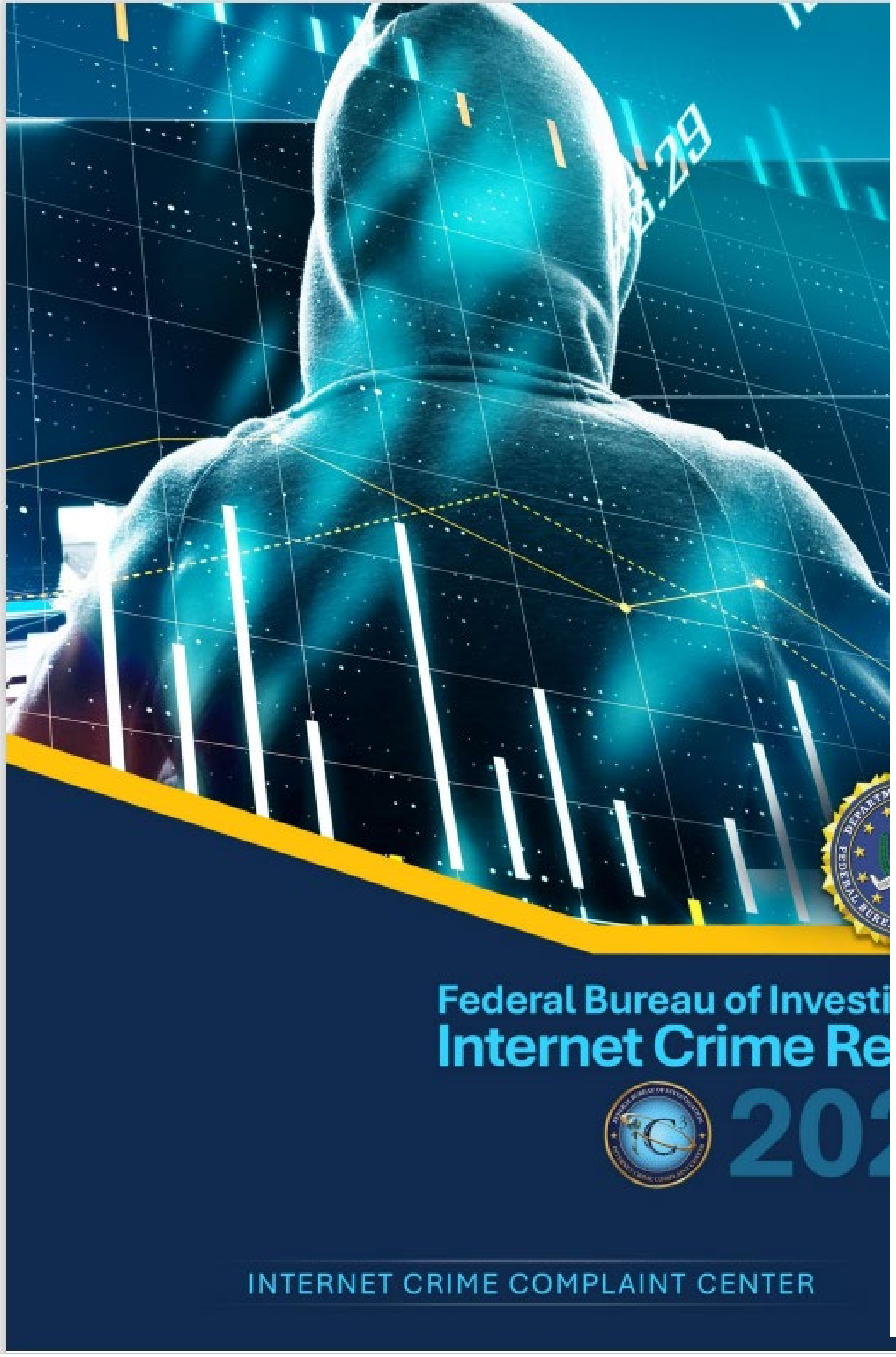
We no longer negotiate with victims. You have 10 days from the receipt of this letter to pay. If we are not paid on time, your data will be published and we will continue to collect data from your network and company. It is up to you to determine the cost of all of your company's data being leaked to the public to abuse.

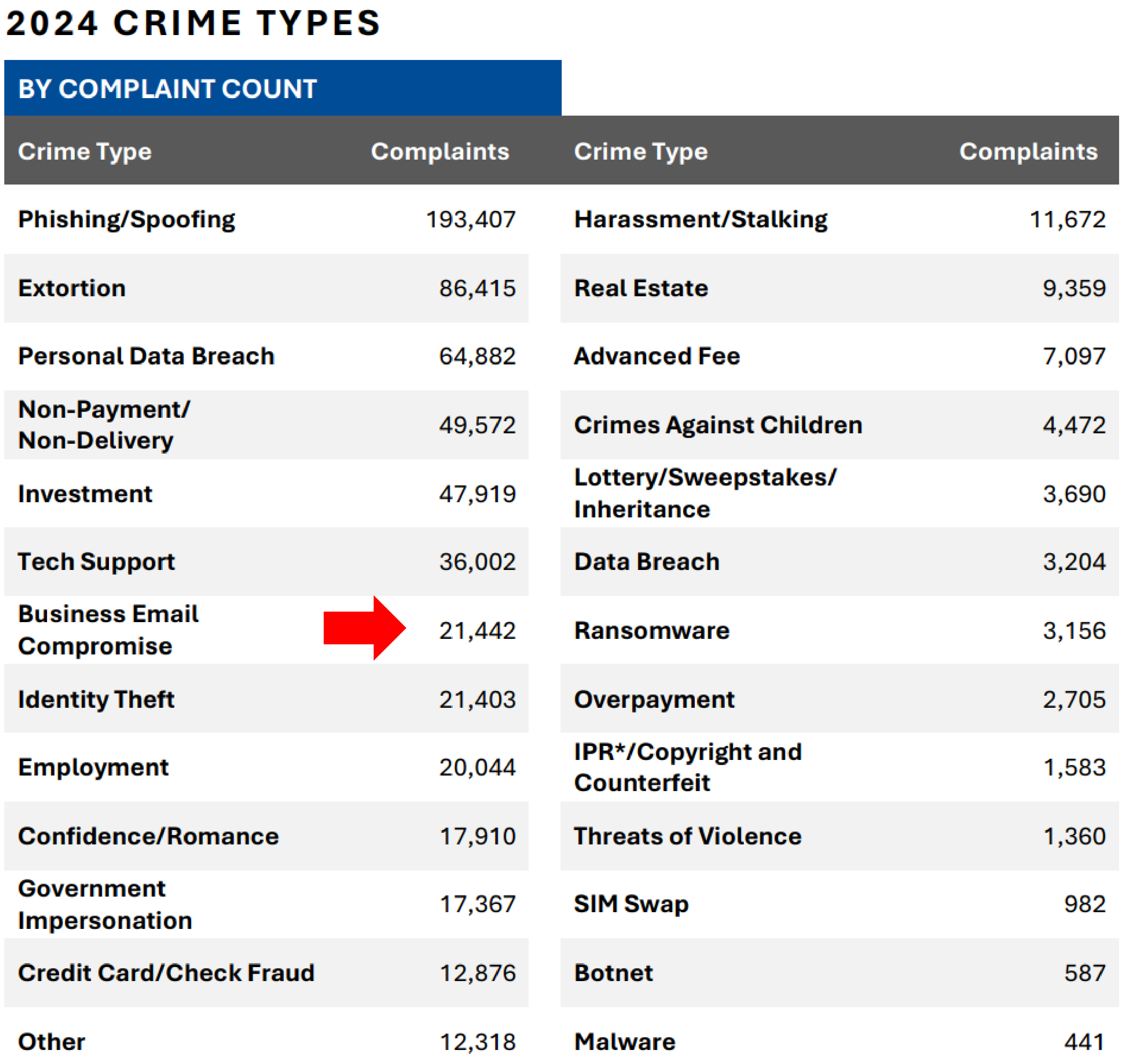
Sincerely,

BIANLIAN GROUP



Type	Complaints
sment/Stalking	11,672
state	9,359
ced Fee	7,097
s Against Children	4,472
/Sweepstakes/ ance	3,690
reach	3,204
mware	3,156
yment	2,705
opyright and erfeit	1,583
s of Violence	1,360
ap	982
	587
re	441

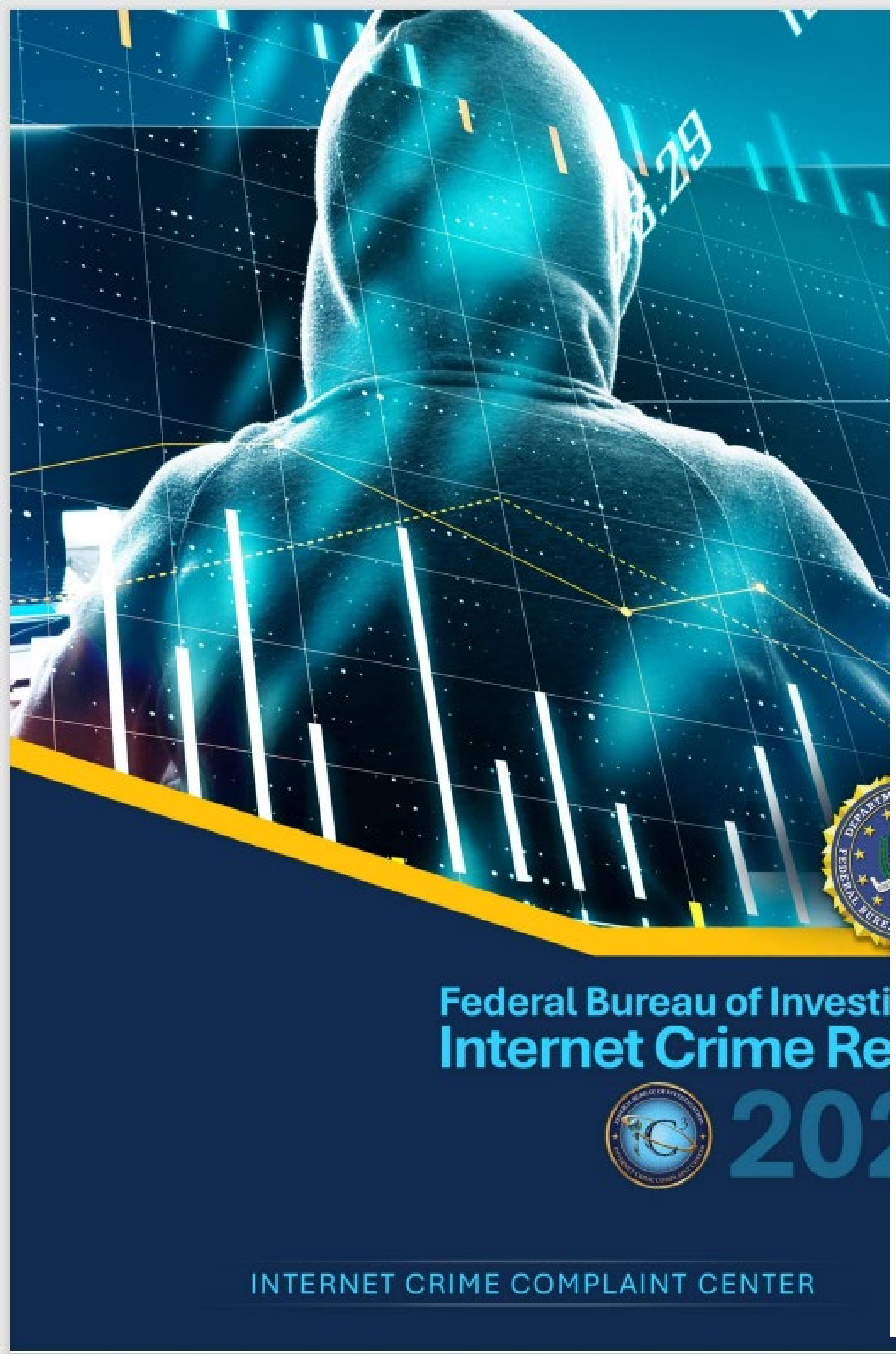


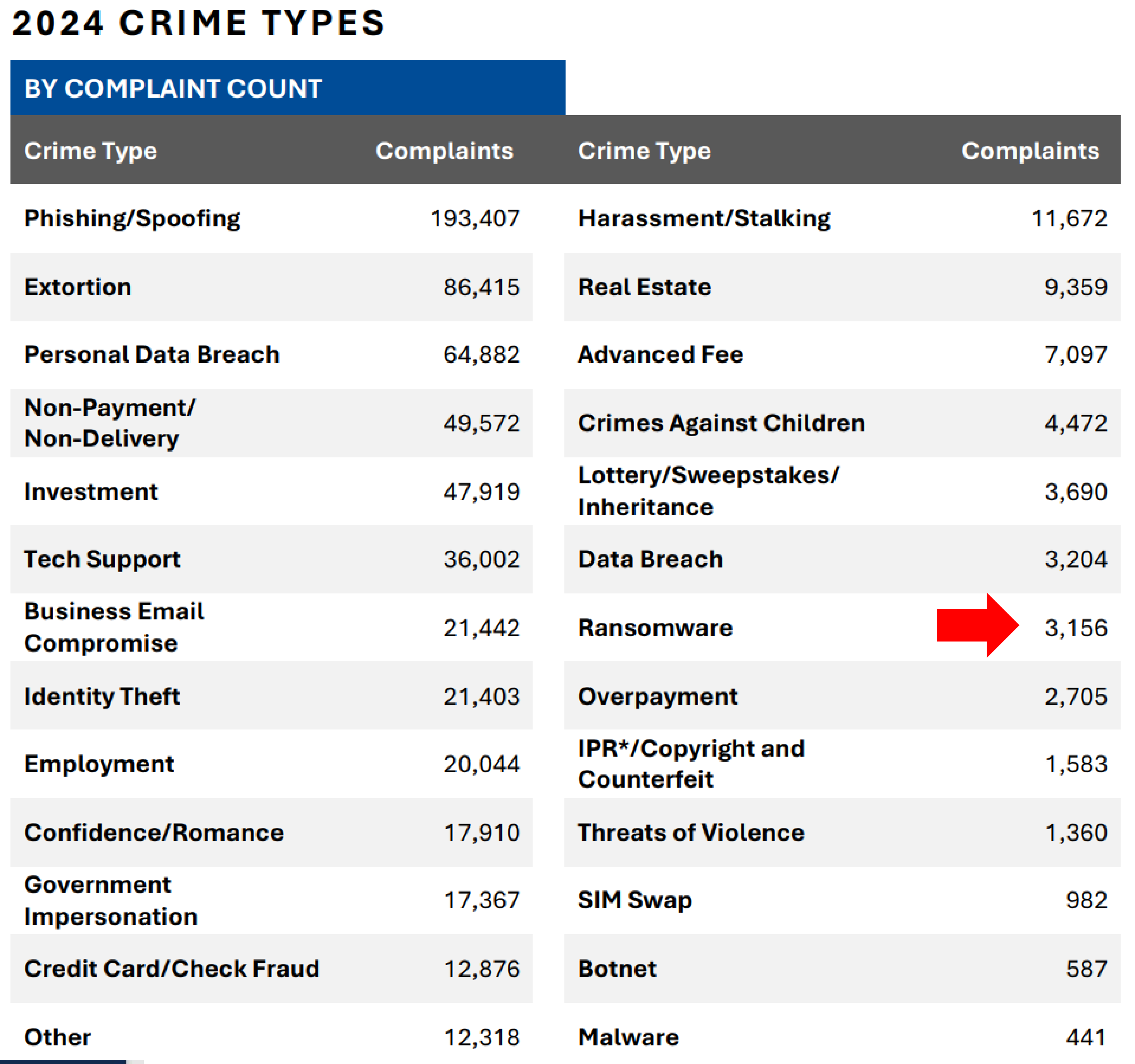


2024 CRIME TYPES

BY COMPLAINT COUNT

Crime Type	Complaints	Crime Type	Complaints
Phishing/Spoofing	193,407	Harassment/Stalking	11,672
Extortion	86,415	Real Estate	9,359
Personal Data Breach	64,882	Advanced Fee	7,097
Non-Payment/ Non-Delivery	49,572	Crimes Against Children	4,472
Investment	47,919	Lottery/Sweepstakes/ Inheritance	3,690
Tech Support	36,002	Data Breach	3,204
Business Email Compromise	➡ 21,442	Ransomware	3,156
Identity Theft	21,403	Overpayment	2,705
Employment	20,044	IPR*/Copyright and Counterfeit	1,583
Confidence/Romance	17,910	Threats of Violence	1,360
Government Impersonation	17,367	SIM Swap	982
Credit Card/Check Fraud	12,876	Botnet	587
Other	12,318	Malware	441

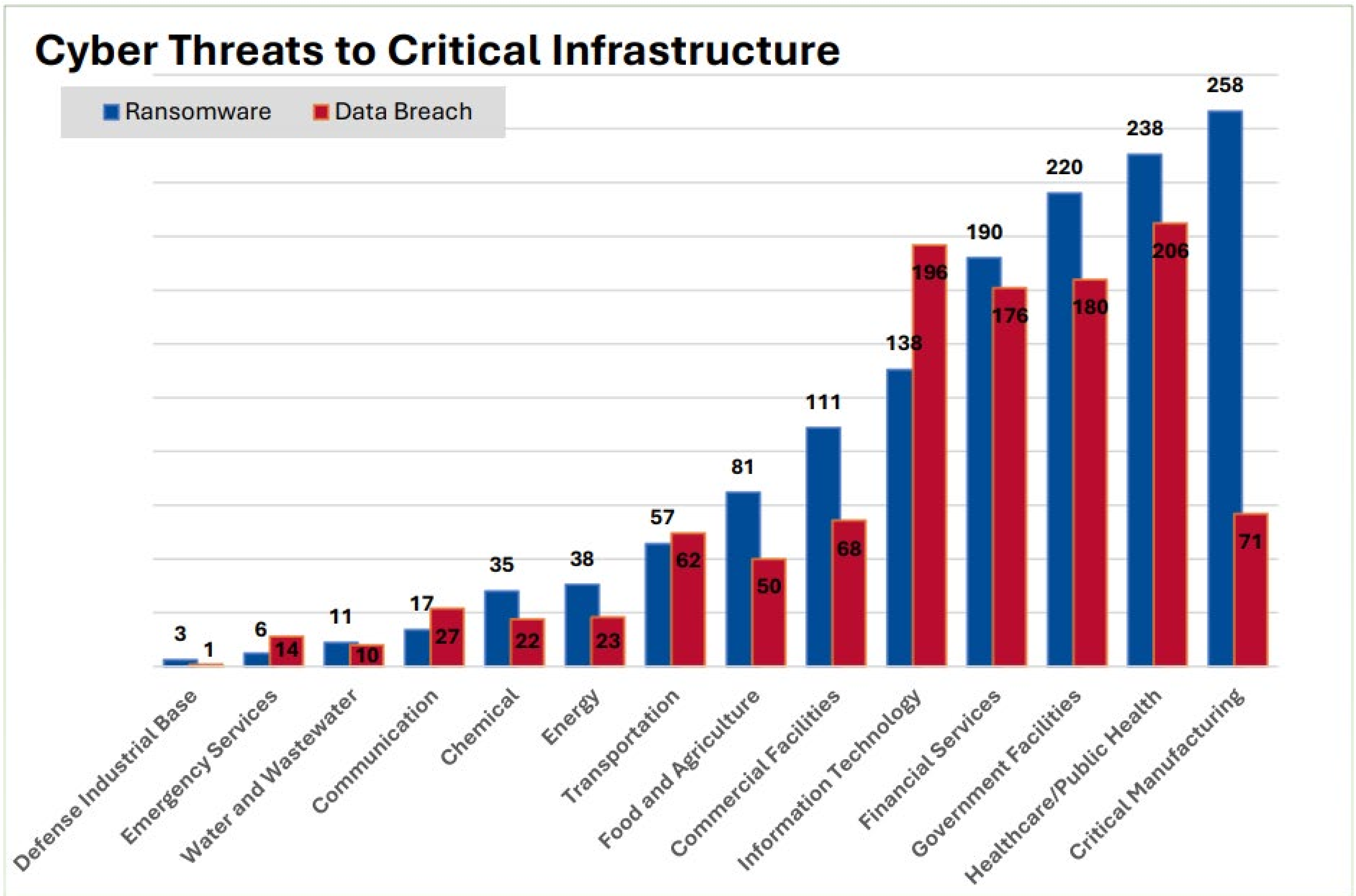




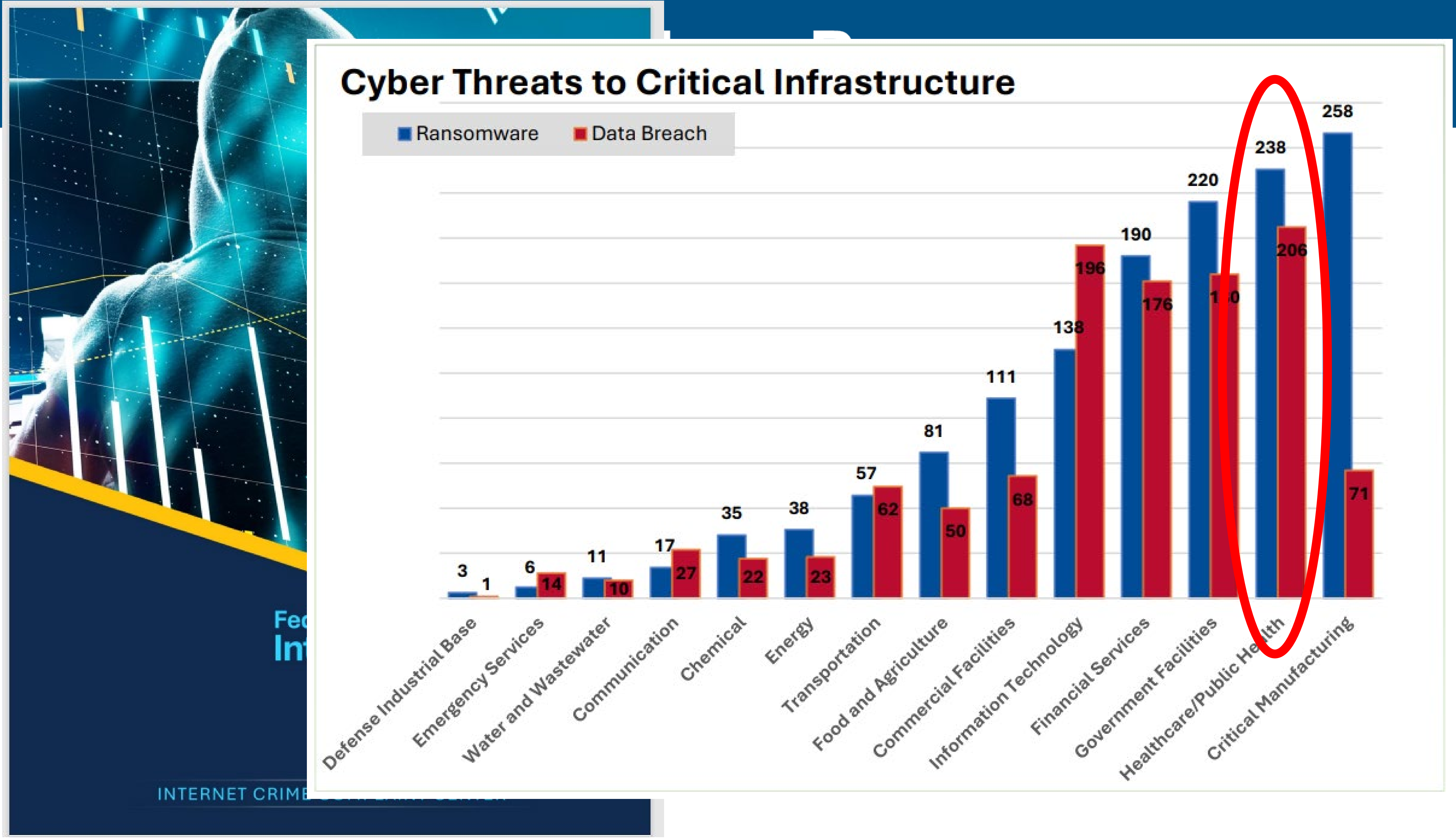
2024 CRIME TYPES

BY COMPLAINT COUNT

Crime Type	Complaints	Crime Type	Complaints
Phishing/Spoofing	193,407	Harassment/Stalking	11,672
Extortion	86,415	Real Estate	9,359
Personal Data Breach	64,882	Advanced Fee	7,097
Non-Payment/ Non-Delivery	49,572	Crimes Against Children	4,472
Investment	47,919	Lottery/Sweepstakes/ Inheritance	3,690
Tech Support	36,002	Data Breach	3,204
Business Email Compromise	21,442	Ransomware	3,156
Identity Theft	21,403	Overpayment	2,705
Employment	20,044	IPR*/Copyright and Counterfeit	1,583
Confidence/Romance	17,910	Threats of Violence	1,360
Government Impersonation	17,367	SIM Swap	982
Credit Card/Check Fraud	12,876	Botnet	587
Other	12,318	Malware	441

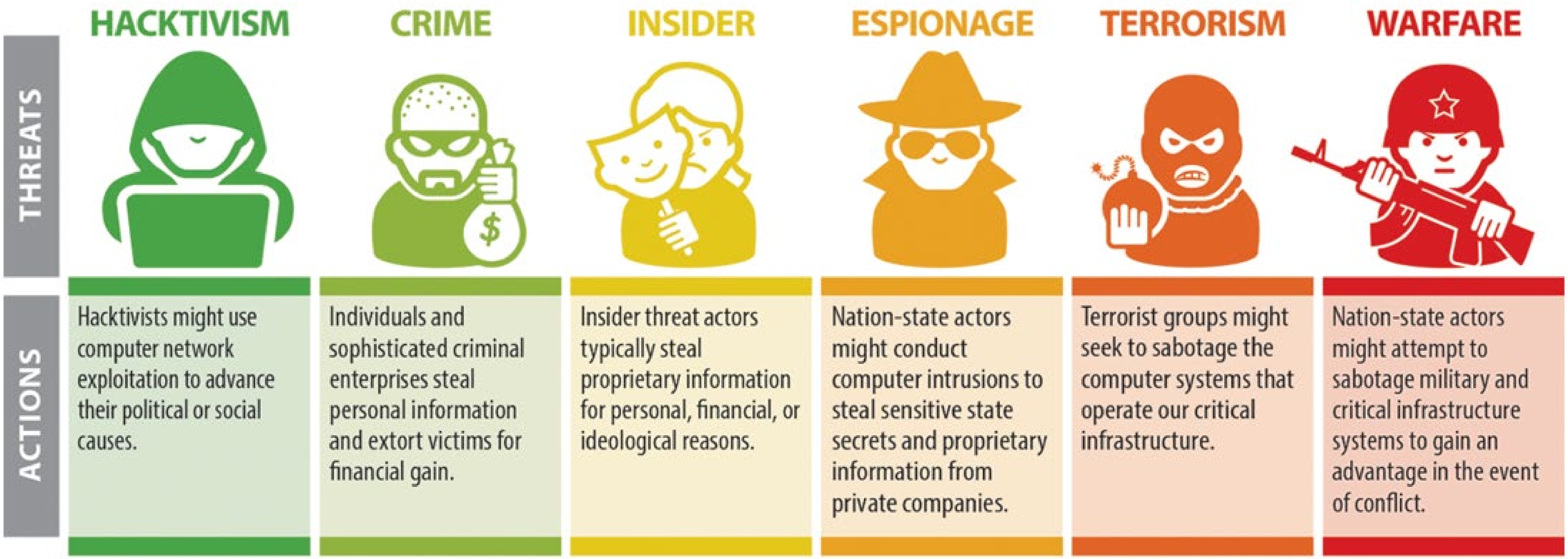


Cyber Threats to Critical Infrastructure



Cyber Threats to Critical Infrastructure

Cyber Threats



	HACKTIVISM	CRIME	INSIDER	ESPIONAGE	TERRORISM	WARFARE
THREATS						
ACTIONS	Hacktivists might use computer network exploitation to advance their political or social causes.	Individuals and sophisticated criminal enterprises steal personal information and extort victims for financial gain.	Insider threat actors typically steal proprietary information for personal, financial, or ideological reasons.	Nation-state actors might conduct computer intrusions to steal sensitive state secrets and proprietary information from private companies.	Terrorist groups might seek to sabotage the computer systems that operate our critical infrastructure.	Nation-state actors might attempt to sabotage military and critical infrastructure systems to gain an advantage in the event of conflict.

2024 ODNI Annual Threat Assessment

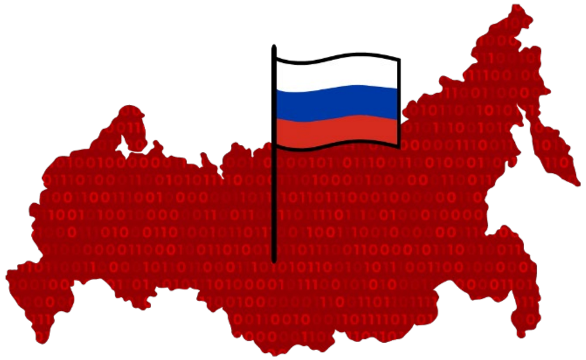
Foreign Threat Actors

PEOPLE'S REPUBLIC OF CHINA

"China remains the most active and persistent cyber threat to U.S. Government, private-sector, and critical infrastructure networks."

IRAN

"Iran's growing expertise and willingness to conduct aggressive cyber operations make it a major threat to the security of U.S. and allied and partner networks and data."



RUSSIA

"Russia will pose an enduring global cyber threat even as it prioritizes cyber operations for the Ukrainian war."

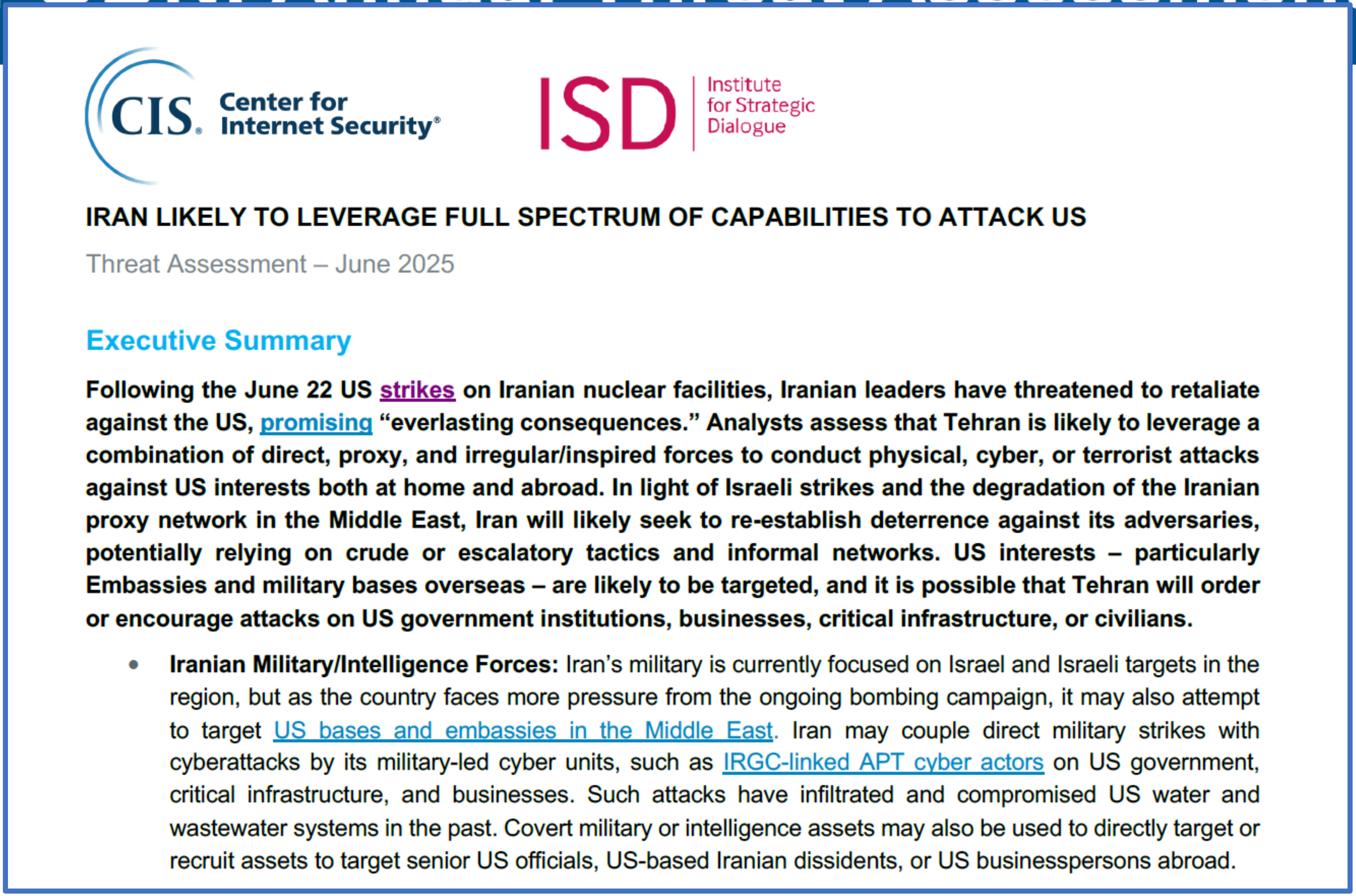
2024 ODNI Annual Threat Assessment

Foreign Threat Actors

IRAN

"Iran's growing expertise and willingness to conduct aggressive cyber operations make it a major threat to the security of U.S. and allied and partner networks and data."

2024 ODNI Annual Threat Assessment



CIS Center for Internet Security®

ISD Institute for Strategic Dialogue

IRAN LIKELY TO LEVERAGE FULL SPECTRUM OF CAPABILITIES TO ATTACK US

Threat Assessment – June 2025

Executive Summary

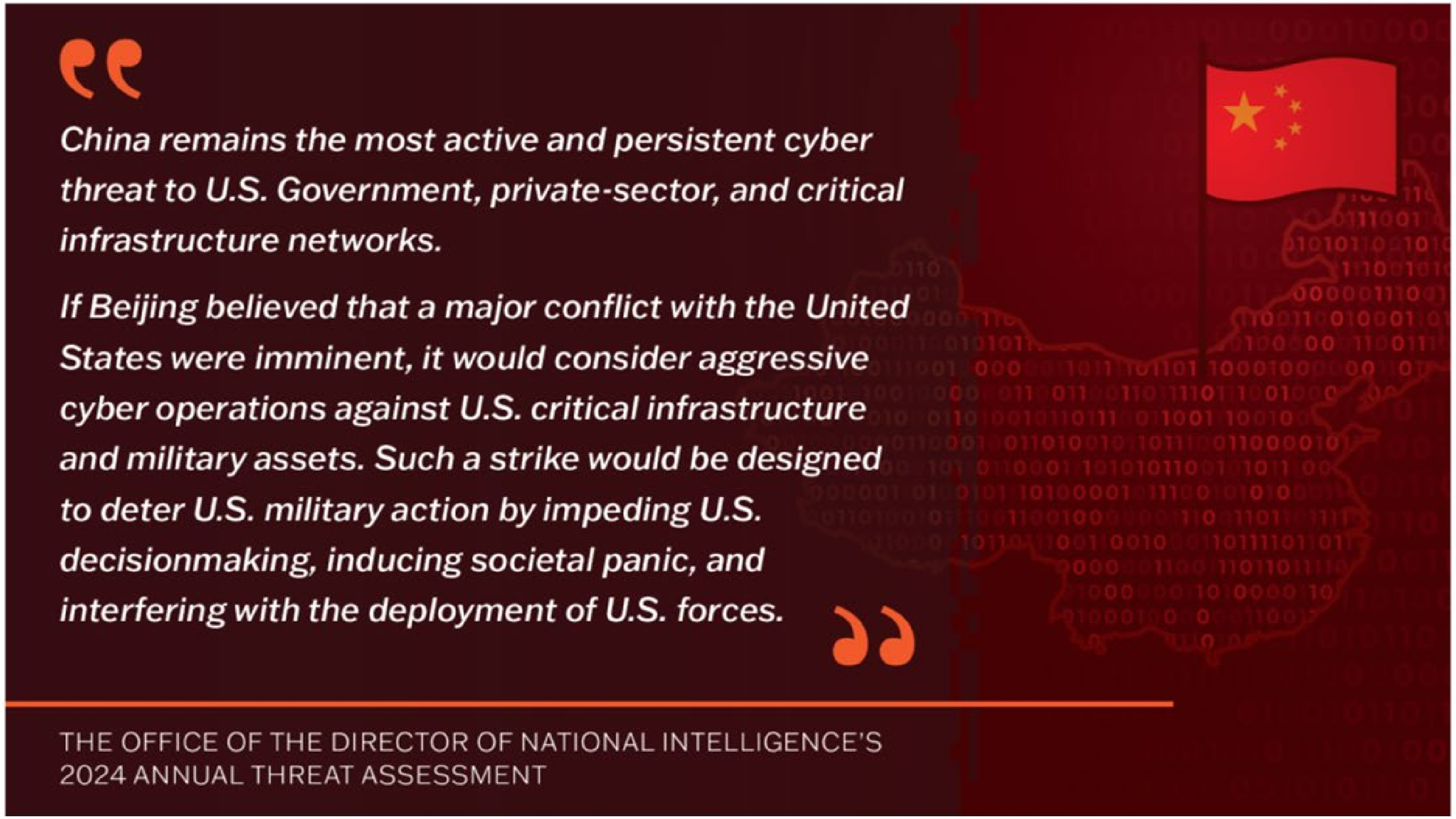
Following the June 22 US strikes on Iranian nuclear facilities, Iranian leaders have threatened to retaliate against the US, promising "everlasting consequences." Analysts assess that Tehran is likely to leverage a combination of direct, proxy, and irregular/inspired forces to conduct physical, cyber, or terrorist attacks against US interests both at home and abroad. In light of Israeli strikes and the degradation of the Iranian proxy network in the Middle East, Iran will likely seek to re-establish deterrence against its adversaries, potentially relying on crude or escalatory tactics and informal networks. US interests – particularly Embassies and military bases overseas – are likely to be targeted, and it is possible that Tehran will order or encourage attacks on US government institutions, businesses, critical infrastructure, or civilians.

- **Iranian Military/Intelligence Forces:** Iran's military is currently focused on Israel and Israeli targets in the region, but as the country faces more pressure from the ongoing bombing campaign, it may also attempt to target US bases and embassies in the Middle East. Iran may couple direct military strikes with cyberattacks by its military-led cyber units, such as IRGC-linked APT cyber actors on US government, critical infrastructure, and businesses. Such attacks have infiltrated and compromised US water and wastewater systems in the past. Covert military or intelligence assets may also be used to directly target or recruit assets to target senior US officials, US-based Iranian dissidents, or US businesspersons abroad.

2024 ODNI Annual Threat Assessment

PEOPLE’S REPUBLIC OF CHINA

“China remains the most active and persistent cyber threat to U.S. Government, private-sector, and critical infrastructure networks.”



China remains the most active and persistent cyber threat to U.S. Government, private-sector, and critical infrastructure networks.

If Beijing believed that a major conflict with the United States were imminent, it would consider aggressive cyber operations against U.S. critical infrastructure and military assets. Such a strike would be designed to deter U.S. military action by impeding U.S. decisionmaking, inducing societal panic, and interfering with the deployment of U.S. forces.

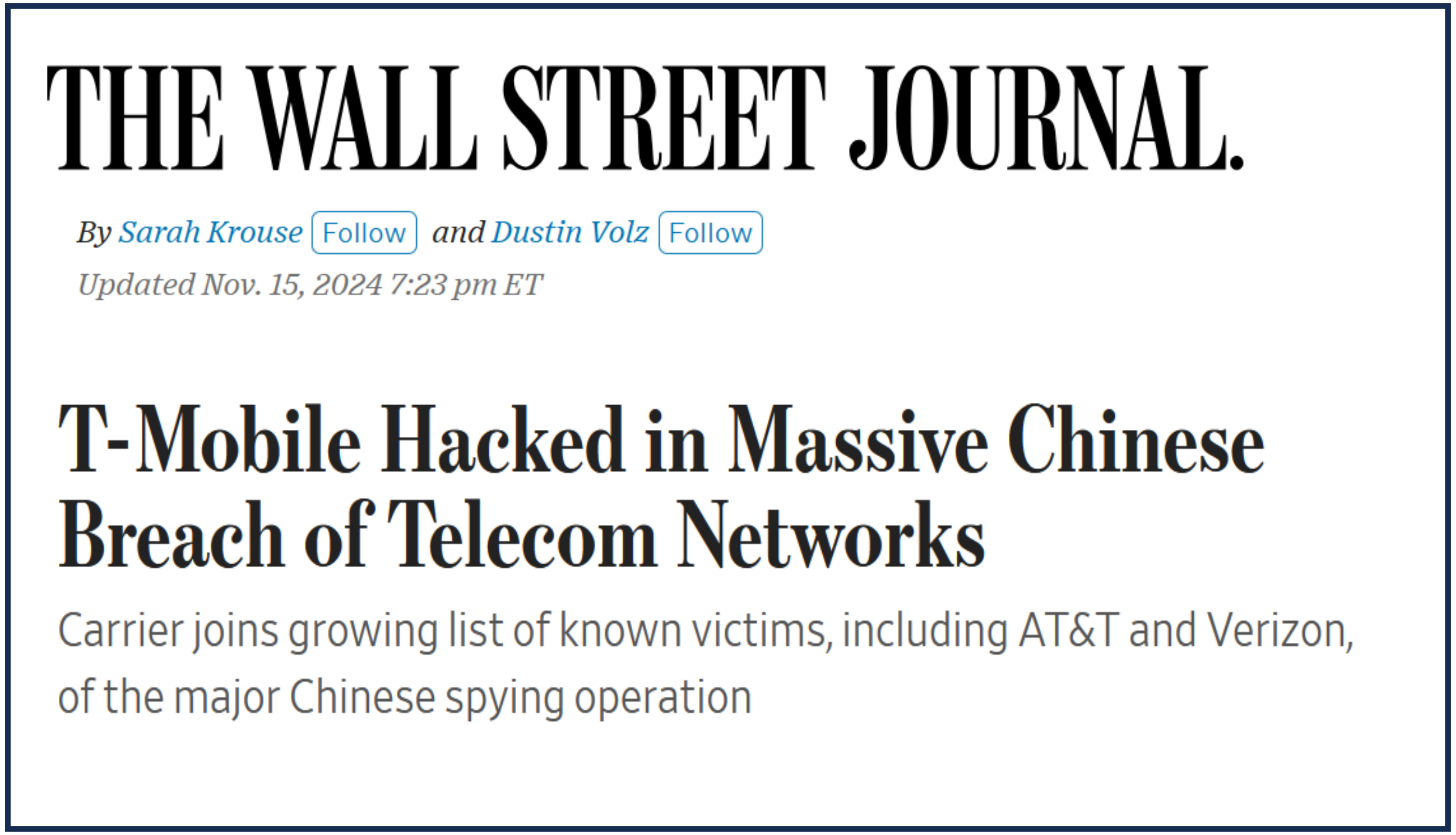
THE OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE’S 2024 ANNUAL THREAT ASSESSMENT

https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors/china

2024 ODNI Annual Threat Assessment

PEOPLE'S REPUBLIC OF CHINA

"China remains the most active and persistent cyber threat to U.S. Government, private-sector, and critical infrastructure networks."



THE WALL STREET JOURNAL.

By Sarah Krouse Follow *and Dustin Volz* Follow

Updated Nov. 15, 2024 7:23 pm ET

T-Mobile Hacked in Massive Chinese Breach of Telecom Networks

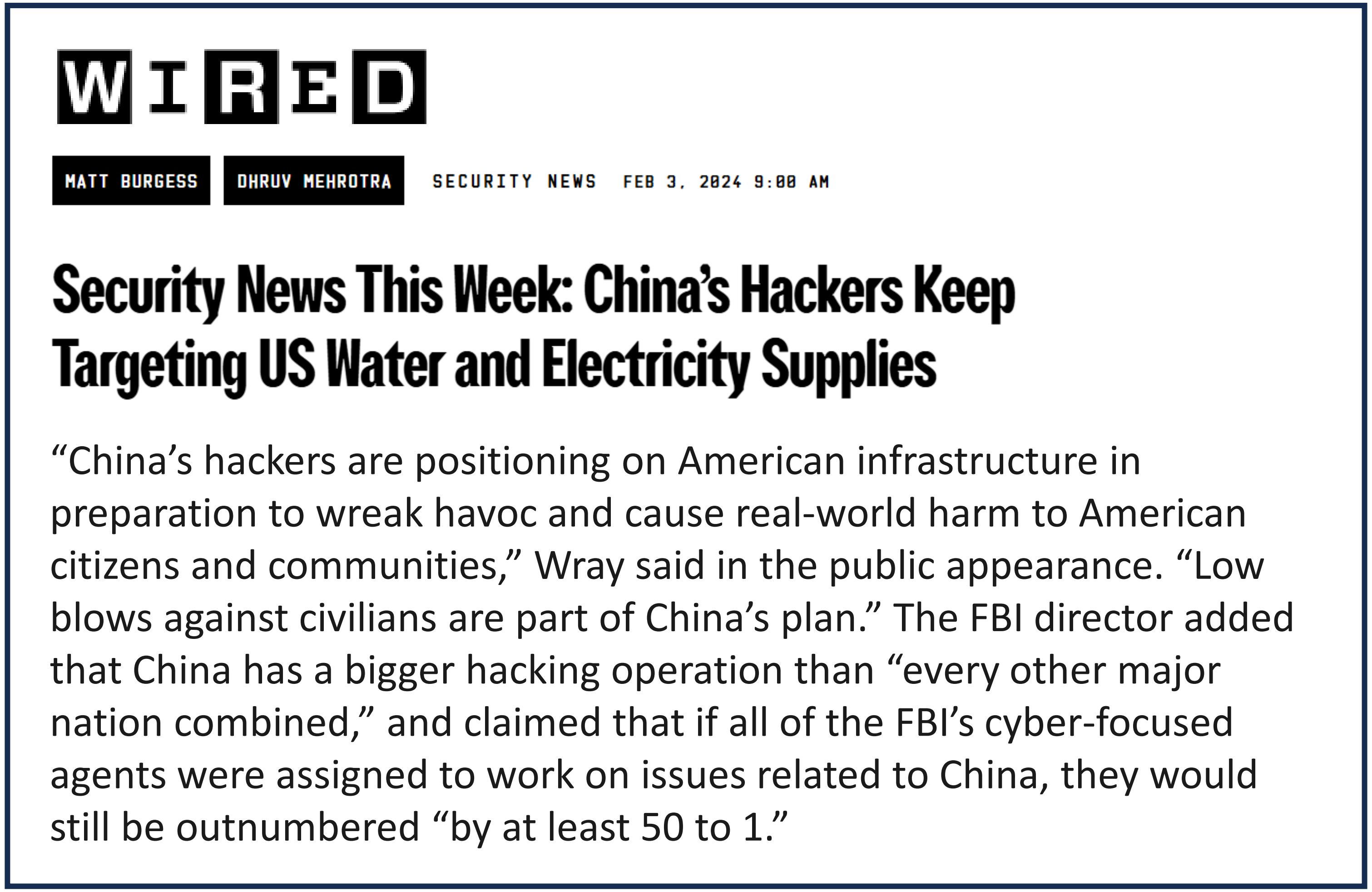
Carrier joins growing list of known victims, including AT&T and Verizon, of the major Chinese spying operation

https://www.wsj.com/politics/national-security/t-mobile-hacked-in-massive-chinese-breach-of-telecom-networks-4b2d7f92

2024 ODNI Annual Threat Assessment

PEOPLE’S REPUBLIC OF CHINA

“China remains the most active and persistent cyber threat to U.S. Government, private-sector, and critical infrastructure networks.”



WIRED

MATT BURGESS DHRUV MEHROTRA SECURITY NEWS FEB 3, 2024 9:00 AM

Security News This Week: China’s Hackers Keep Targeting US Water and Electricity Supplies

“China’s hackers are positioning on American infrastructure in preparation to wreak havoc and cause real-world harm to American citizens and communities,” Wray said in the public appearance. “Low blows against civilians are part of China’s plan.” The FBI director added that China has a bigger hacking operation than “every other major nation combined,” and claimed that if all of the FBI’s cyber-focused agents were assigned to work on issues related to China, they would still be outnumbered “by at least 50 to 1.”

China’s Hackers Keep Targeting US Water and Electricity Supplies | WIRED

Ransomware Hardening

1. Train ALL Employees on Cybersecurity Awareness

Ransomware Hardening

1. Train ALL Employees on Cybersecurity Awareness

2. Implement Multi-Factor / Advanced Authentication

Ransomware Hardening

1. Train ALL Employees on Cybersecurity Awareness

2. Implement Multi-Factor / Advanced Authentication

3. Install Software Updates & Patches Regularly

Disruptive Technology: AI Threats

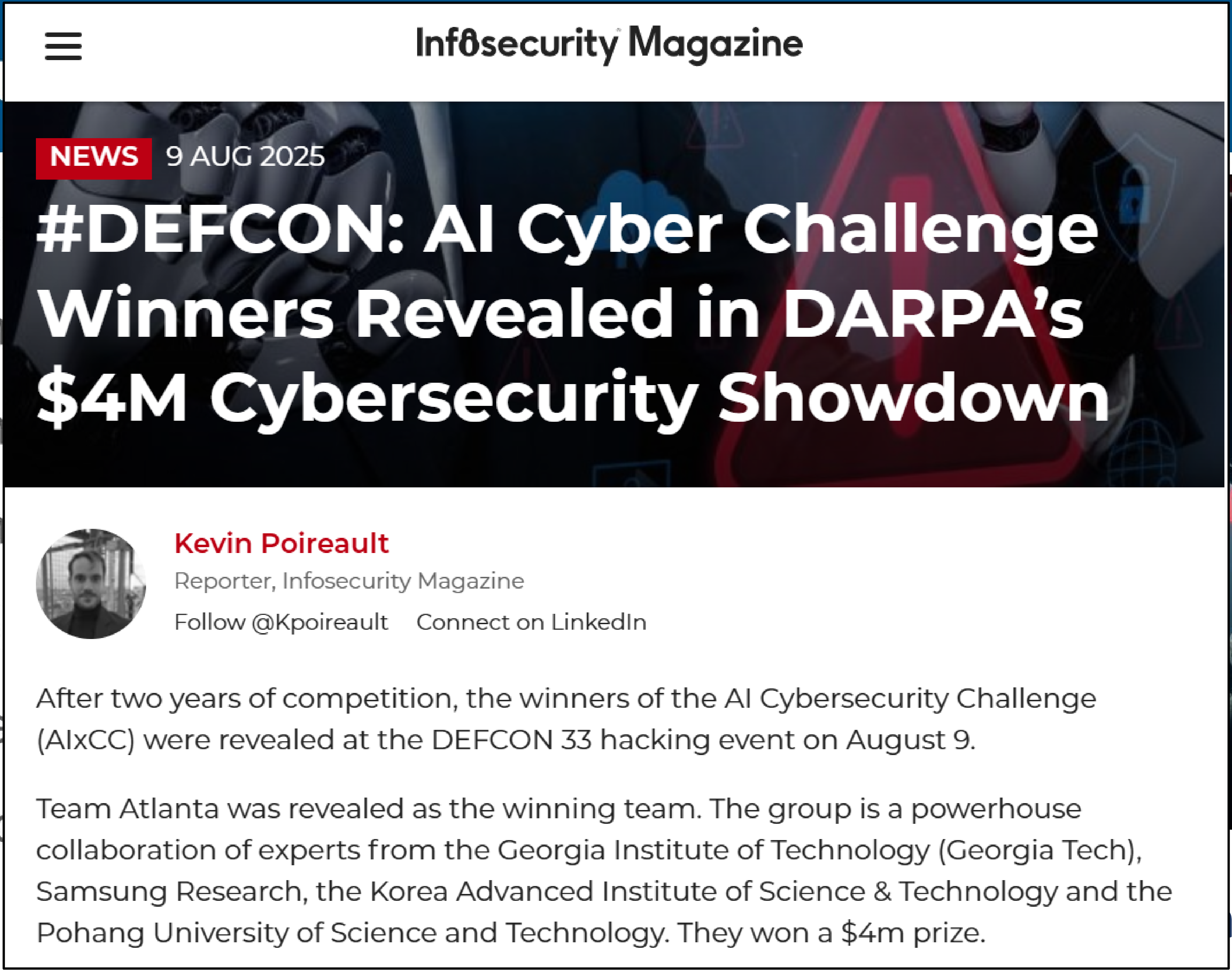
- Attacks on AI Systems
- AI Enabled Phishing
- AI Enabled Vulnerability Research
- AI Enabled Hacking
- Used to Create Disinformation
- Voice & Video Cloning
- Breach AI Guardrails

Disruptive Technology: AI Threats

- Attacks on AI Systems
- AI Enabled Phishing
- ➡ AI Enabled Vulnerability Research
- AI Enabled Hacking
- Used to Create Disinformation
- Voice & Video Cloning
- Breach AI Guardrails

Disru

- Attac
- AI En
- AI En
- AI En
- Used
- Voice
- Breac



Inf0security Magazine

NEWS 9 AUG 2025

#DEFCON: AI Cyber Challenge Winners Revealed in DARPA's $4M Cybersecurity Showdown

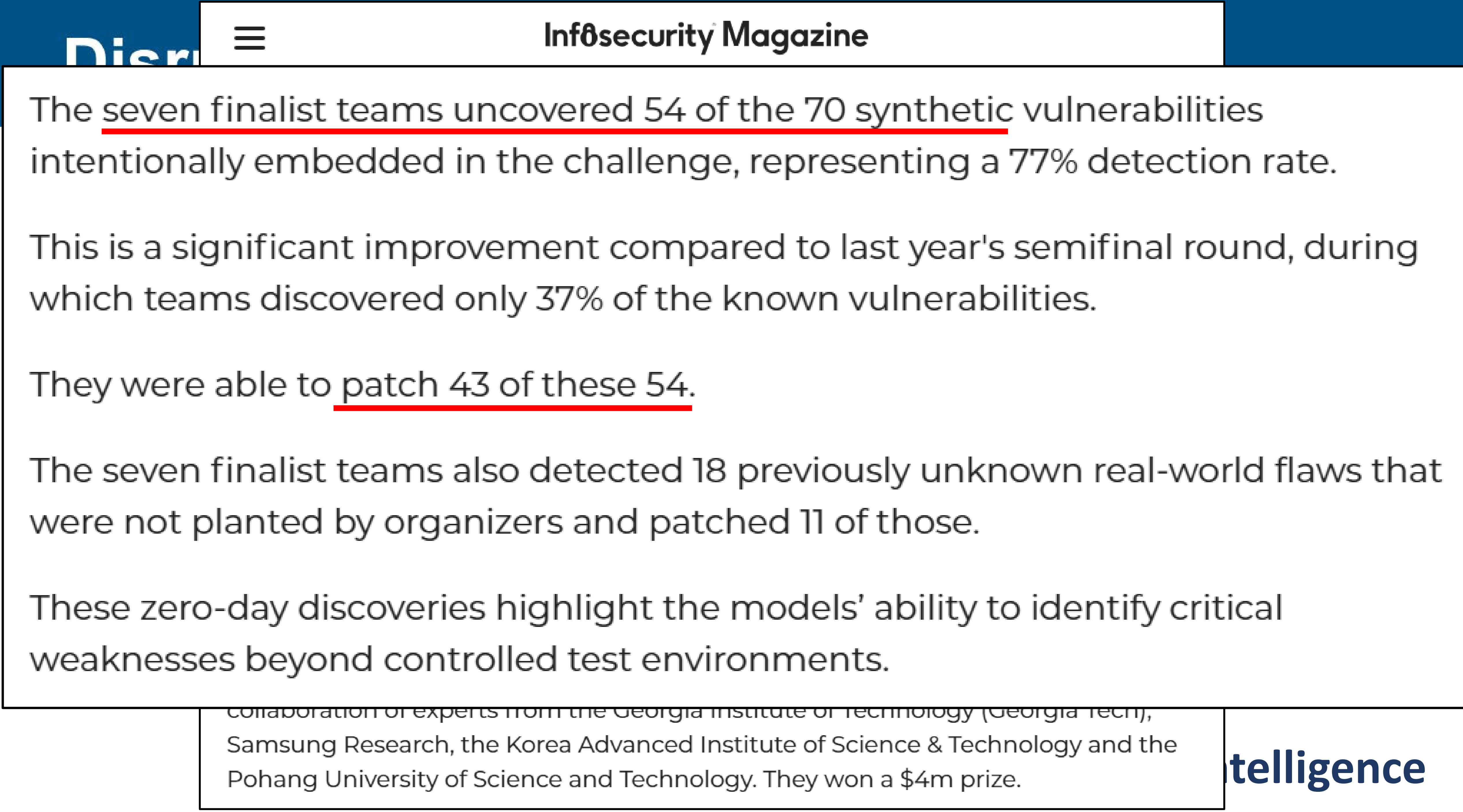
Kevin Poireault
Reporter, Infosecurity Magazine
Follow @Kpoireault Connect on LinkedIn

After two years of competition, the winners of the AI Cybersecurity Challenge (AIxCC) were revealed at the DEFCON 33 hacking event on August 9.

Team Atlanta was revealed as the winning team. The group is a powerhouse collaboration of experts from the Georgia Institute of Technology (Georgia Tech), Samsung Research, the Korea Advanced Institute of Science & Technology and the Pohang University of Science and Technology. They won a $4m prize.

telligence

Disr



Inf0security Magazine

The seven finalist teams uncovered 54 of the 70 synthetic vulnerabilities intentionally embedded in the challenge, representing a 77% detection rate.

This is a significant improvement compared to last year's semifinal round, during which teams discovered only 37% of the known vulnerabilities.

They were able to patch 43 of these 54.

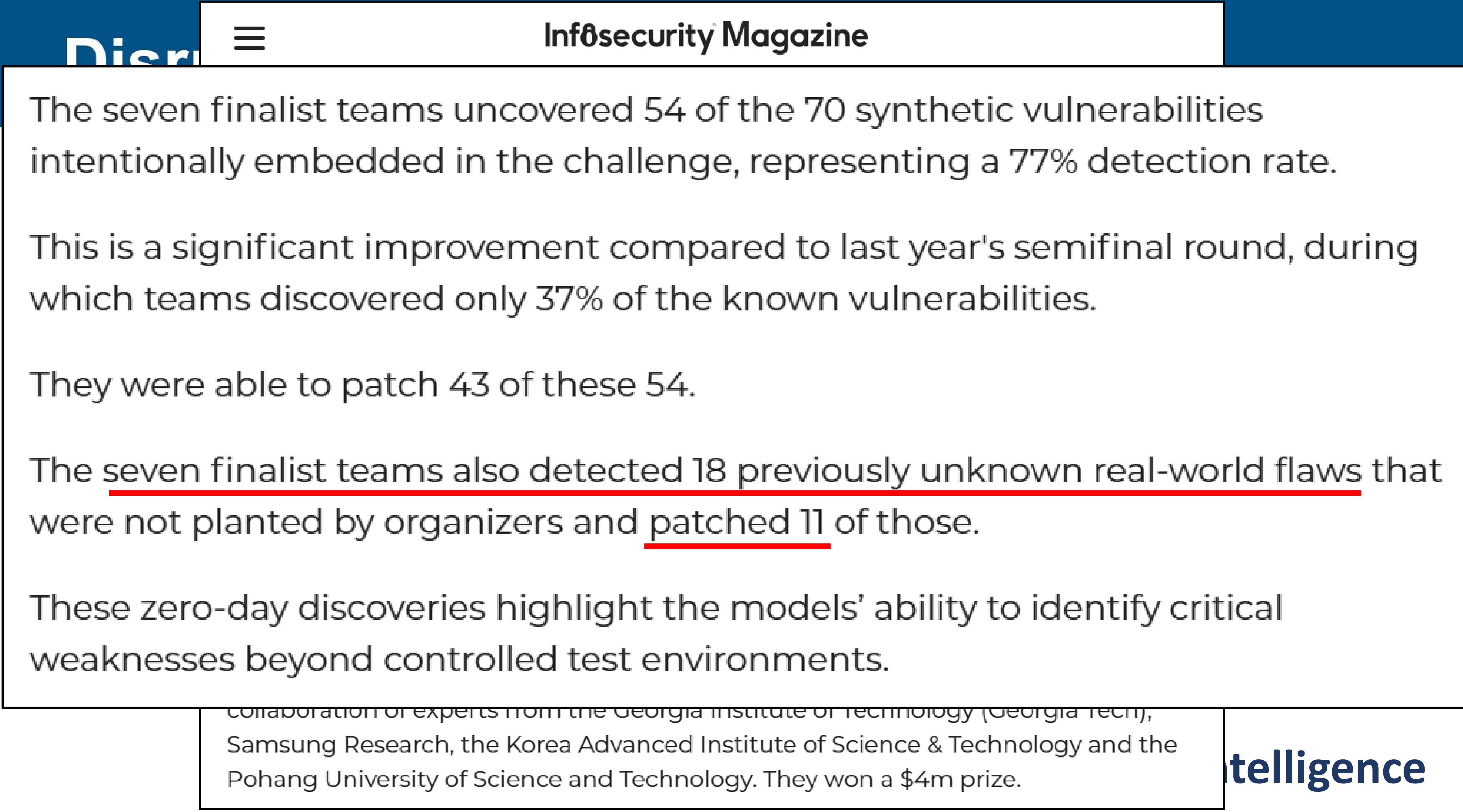
The seven finalist teams also detected 18 previously unknown real-world flaws that were not planted by organizers and patched 11 of those.

These zero-day discoveries highlight the models' ability to identify critical weaknesses beyond controlled test environments.

collaboration of experts from the Georgia Institute of Technology (Georgia Tech), Samsung Research, the Korea Advanced Institute of Science & Technology and the Pohang University of Science and Technology. They won a $4m prize.

telligence

Disr



Inf0security Magazine

The seven finalist teams uncovered 54 of the 70 synthetic vulnerabilities intentionally embedded in the challenge, representing a 77% detection rate.

This is a significant improvement compared to last year's semifinal round, during which teams discovered only 37% of the known vulnerabilities.

They were able to patch 43 of these 54.

The seven finalist teams also detected 18 previously unknown real-world flaws that were not planted by organizers and patched 11 of those.

These zero-day discoveries highlight the models' ability to identify critical weaknesses beyond controlled test environments.

collaboration of experts from the Georgia Institute of Technology (Georgia Tech), Samsung Research, the Korea Advanced Institute of Science & Technology and the Pohang University of Science and Technology. They won a $4m prize.

telligence

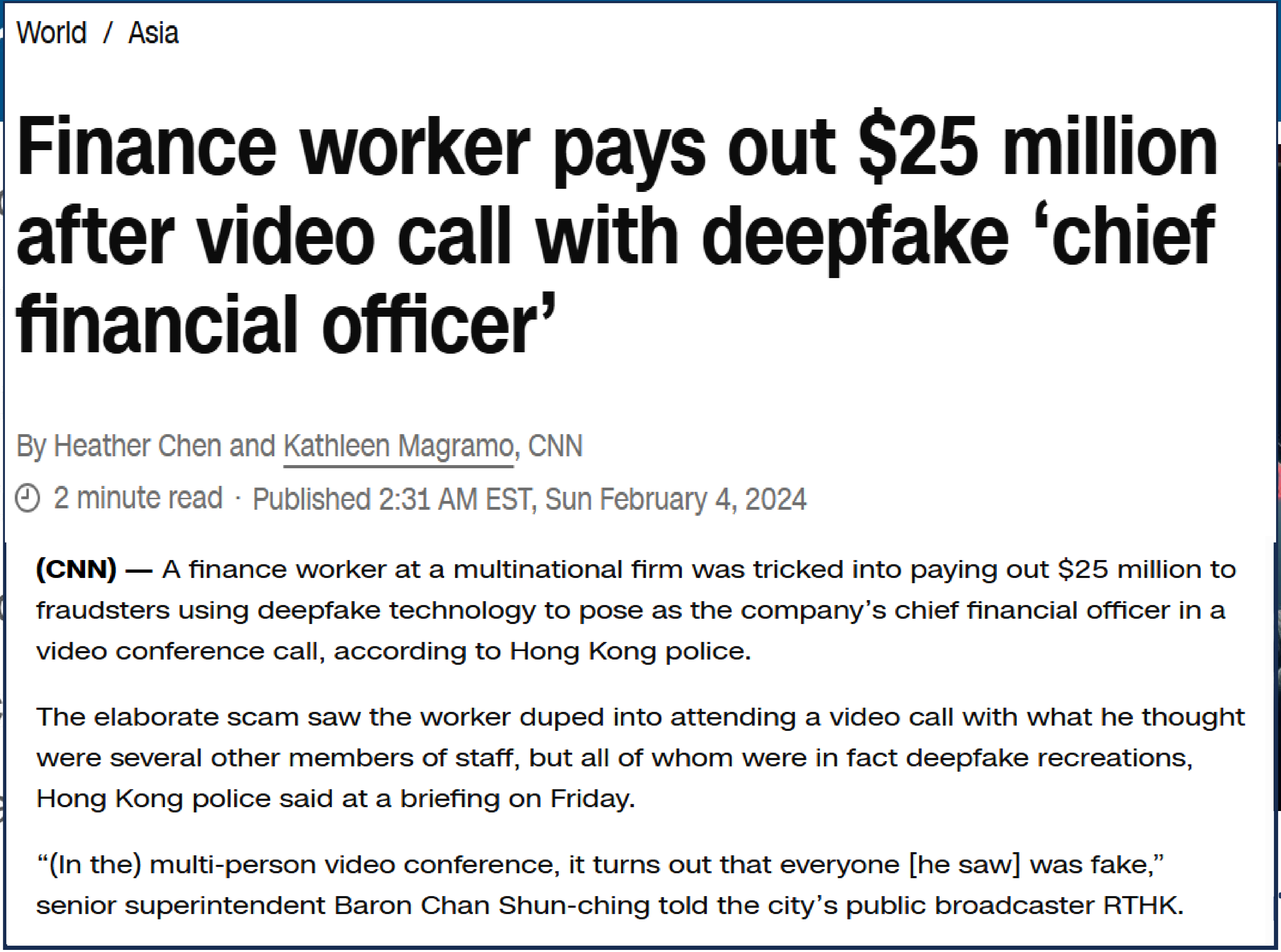
Disruptive Technology: AI Threats

- Attacks on AI Systems
- AI Enabled Phishing
- AI Enabled Vulnerability Research
- AI Enabled Hacking
- Used to Create Disinformation
- ➡ Voice & Video Cloning
- Breach AI Guardrails

Artificial Intelligence

Disr

- Attac
- AI E
- AI E
- AI E
- Usec
- Voic
- Brea



World / Asia

Finance worker pays out $25 million after video call with deepfake 'chief financial officer'

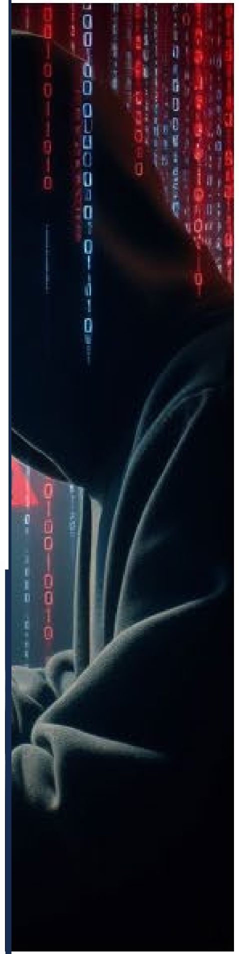
By Heather Chen and Kathleen Magramo, CNN

2 minute read · Published 2:31 AM EST, Sun February 4, 2024

(CNN) — A finance worker at a multinational firm was tricked into paying out $25 million to fraudsters using deepfake technology to pose as the company's chief financial officer in a video conference call, according to Hong Kong police.

The elaborate scam saw the worker duped into attending a video call with what he thought were several other members of staff, but all of whom were in fact deepfake recreations, Hong Kong police said at a briefing on Friday.

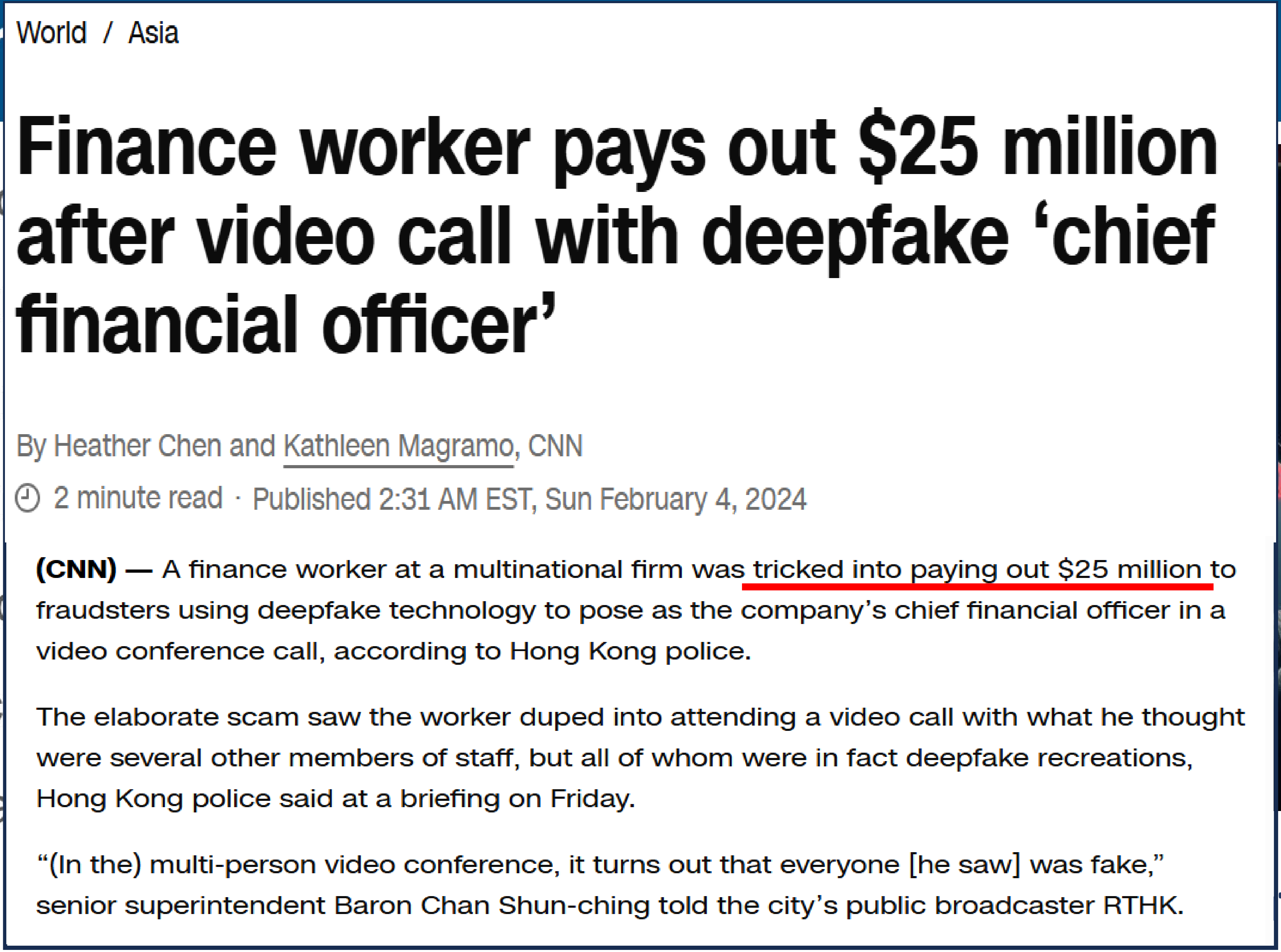
"(In the) multi-person video conference, it turns out that everyone [he saw] was fake," senior superintendent Baron Chan Shun-ching told the city's public broadcaster RTHK.



telligence

Disr

- Attac
- AI E
- AI E
- AI E
- Usec
- Voic
- Brea



World / Asia

Finance worker pays out $25 million after video call with deepfake 'chief financial officer'

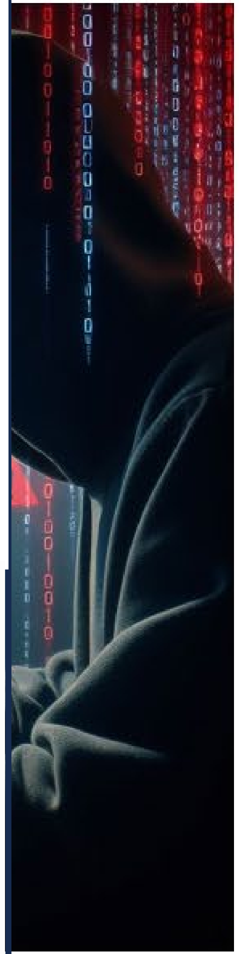
By Heather Chen and Kathleen Magramo, CNN

2 minute read · Published 2:31 AM EST, Sun February 4, 2024

(CNN) — A finance worker at a multinational firm was tricked into paying out $25 million to fraudsters using deepfake technology to pose as the company's chief financial officer in a video conference call, according to Hong Kong police.

The elaborate scam saw the worker duped into attending a video call with what he thought were several other members of staff, but all of whom were in fact deepfake recreations, Hong Kong police said at a briefing on Friday.

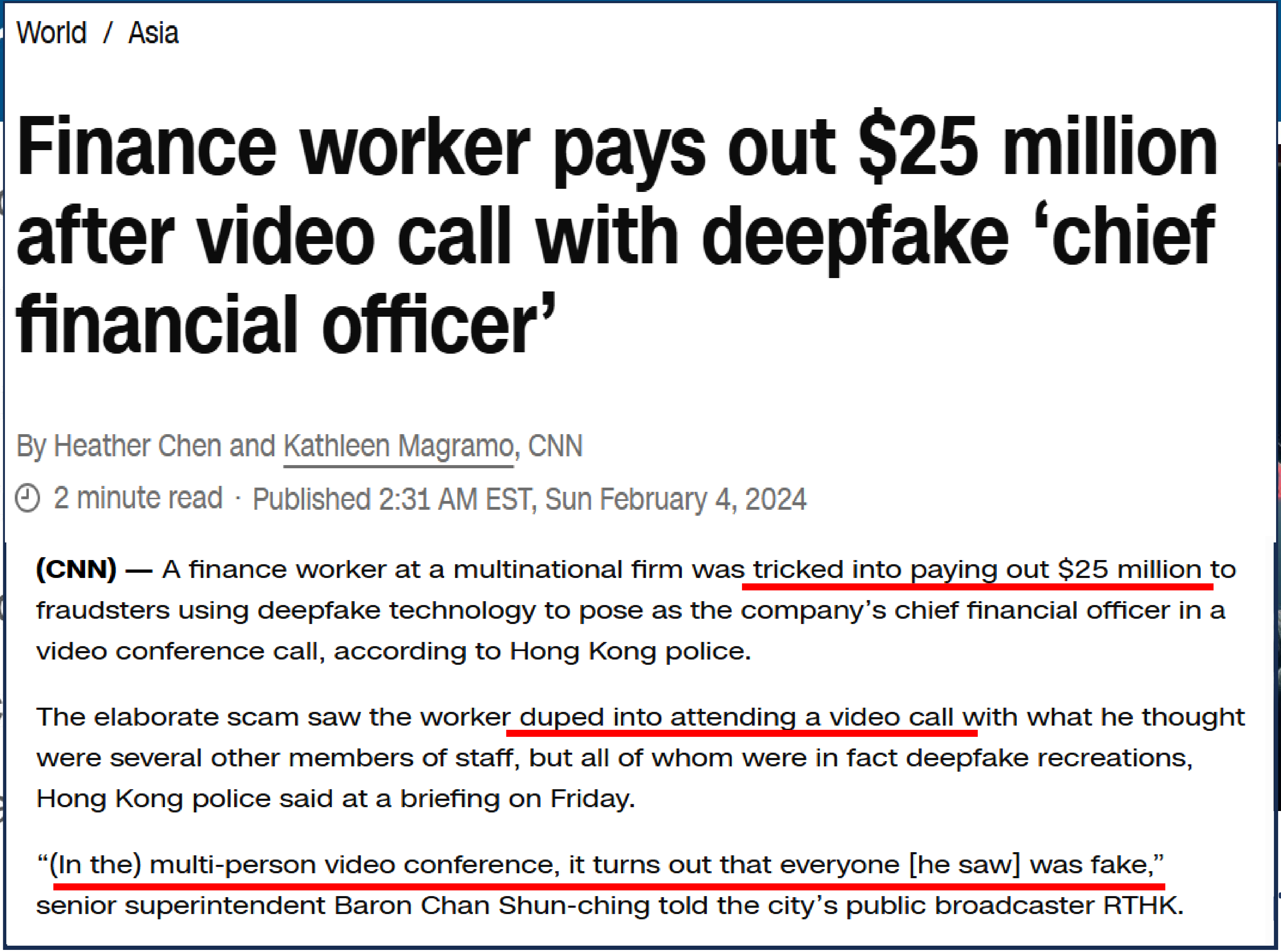
"(In the) multi-person video conference, it turns out that everyone [he saw] was fake," senior superintendent Baron Chan Shun-ching told the city's public broadcaster RTHK.



telligence

Disr

- Attac
- AI E
- AI E
- AI E
- Usec
- Voic
- Brea



World / Asia

Finance worker pays out $25 million after video call with deepfake 'chief financial officer'

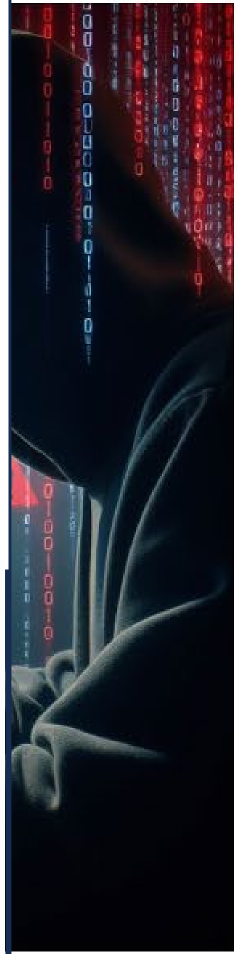
By Heather Chen and Kathleen Magramo, CNN

2 minute read · Published 2:31 AM EST, Sun February 4, 2024

(CNN) — A finance worker at a multinational firm was tricked into paying out $25 million to fraudsters using deepfake technology to pose as the company's chief financial officer in a video conference call, according to Hong Kong police.

The elaborate scam saw the worker duped into attending a video call with what he thought were several other members of staff, but all of whom were in fact deepfake recreations, Hong Kong police said at a briefing on Friday.

"(In the) multi-person video conference, it turns out that everyone [he saw] was fake," senior superintendent Baron Chan Shun-ching told the city's public broadcaster RTHK.

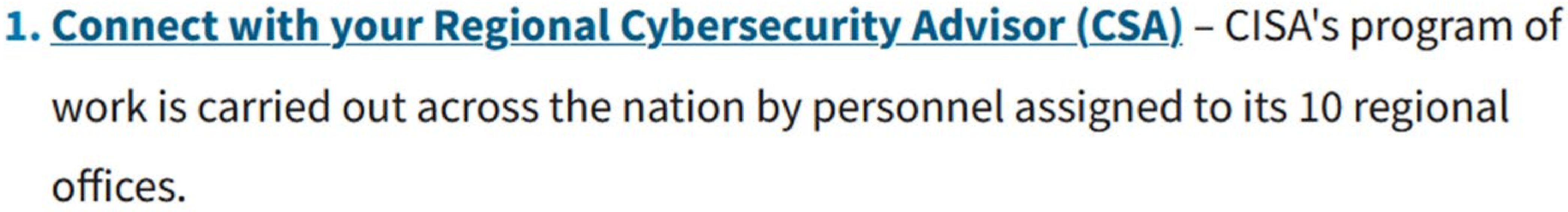


telligence

Disruptive Technology: AI Threats

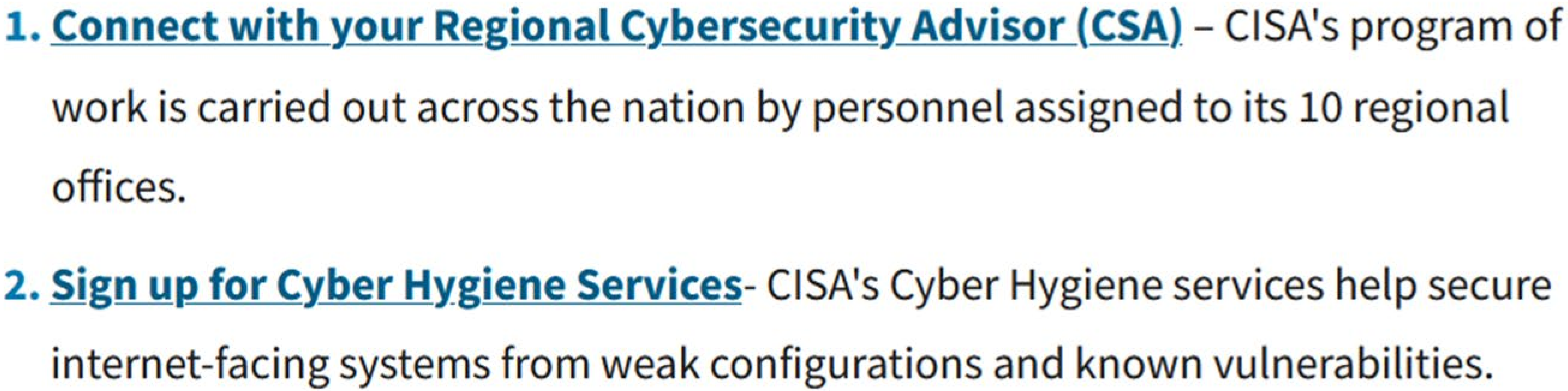
- Attacks on AI Systems
- AI Enabled Phishing
- AI Enabled Vulnerability Research
- AI Enabled Hacking
- Used to Create Disinformation
- Voice & Video Cloning
- Breach AI Guardrails

Take Aways…



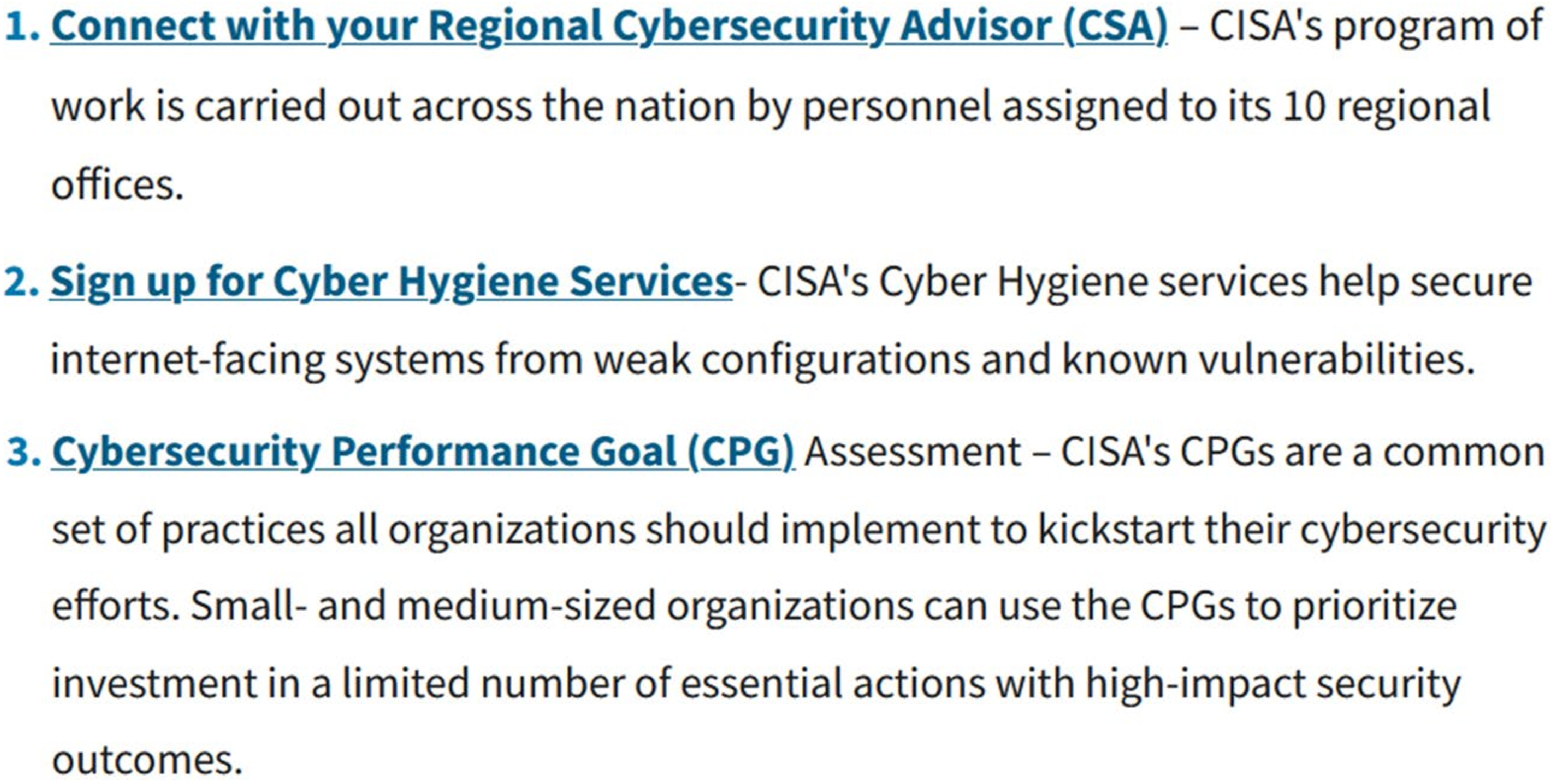
1. **Connect with your Regional Cybersecurity Advisor (CSA)** – CISA's program of work is carried out across the nation by personnel assigned to its 10 regional offices.

Take Aways…



1. **Connect with your Regional Cybersecurity Advisor (CSA)** – CISA's program of work is carried out across the nation by personnel assigned to its 10 regional offices.
2. **Sign up for Cyber Hygiene Services**- CISA's Cyber Hygiene services help secure internet-facing systems from weak configurations and known vulnerabilities.

Take Aways…



1. **Connect with your Regional Cybersecurity Advisor (CSA)** – CISA's program of work is carried out across the nation by personnel assigned to its 10 regional offices.
2. **Sign up for Cyber Hygiene Services**- CISA's Cyber Hygiene services help secure internet-facing systems from weak configurations and known vulnerabilities.
3. **Cybersecurity Performance Goal (CPG)** Assessment – CISA's CPGs are a common set of practices all organizations should implement to kickstart their cybersecurity efforts. Small- and medium-sized organizations can use the CPGs to prioritize investment in a limited number of essential actions with high-impact security outcomes.

Greg Park

CISA – Region 9
Law Enforcement Liaison

Email: greg.park@cisa.dhs.gov

Phone: (202) 394-5283

Greg Park

CISA – Region 9
Law Enforcement Liaison

Email: greg.park@cisa.dhs.gov

Phone: (202) 394-5283