NSA CYBERSECURITY

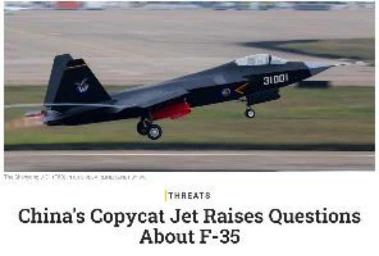
NSA's DIB Cybersecurity Services

NSA CYBERSECURITY COLLABORATION CENTER
2024

THE THREAT LANDSCAPE

Nation-states Target Primes & SMBs

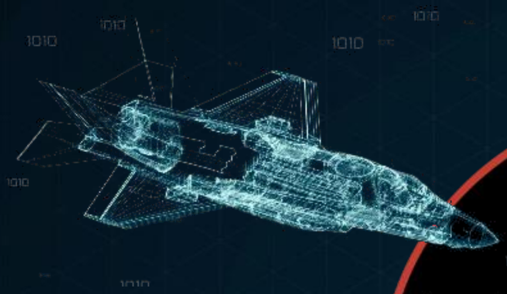
Nation-states are Leveraging U.S. based infrastructure to obfuscate activities



[illegible]

THREATS

China's Copycat Jet Raises Questions About F-35



Ransomware

Disproportionately impacts SMBs

In 2021 **81%** of ransomware attacks were against companies with fewer than 1,000 employees.

55% of consumers in the U.S. would be less likely to continue doing business with companies that are breached.

Exploitation of Internet-facing, publicly known vulnerabilities are the most common attack vector for ransomware

Complexity of the DoD Supply Chain

How Many Contacts Are Truly In Your Network?

25	Prime companies
18,476	Tier two subs
229,562	Tier three subs

Patch Fatigue & Issue Prioritization

Projected

500 CVEs published per week in 2025

The average org has

>100,000 **backlogged** vulnerabilities

~25,000

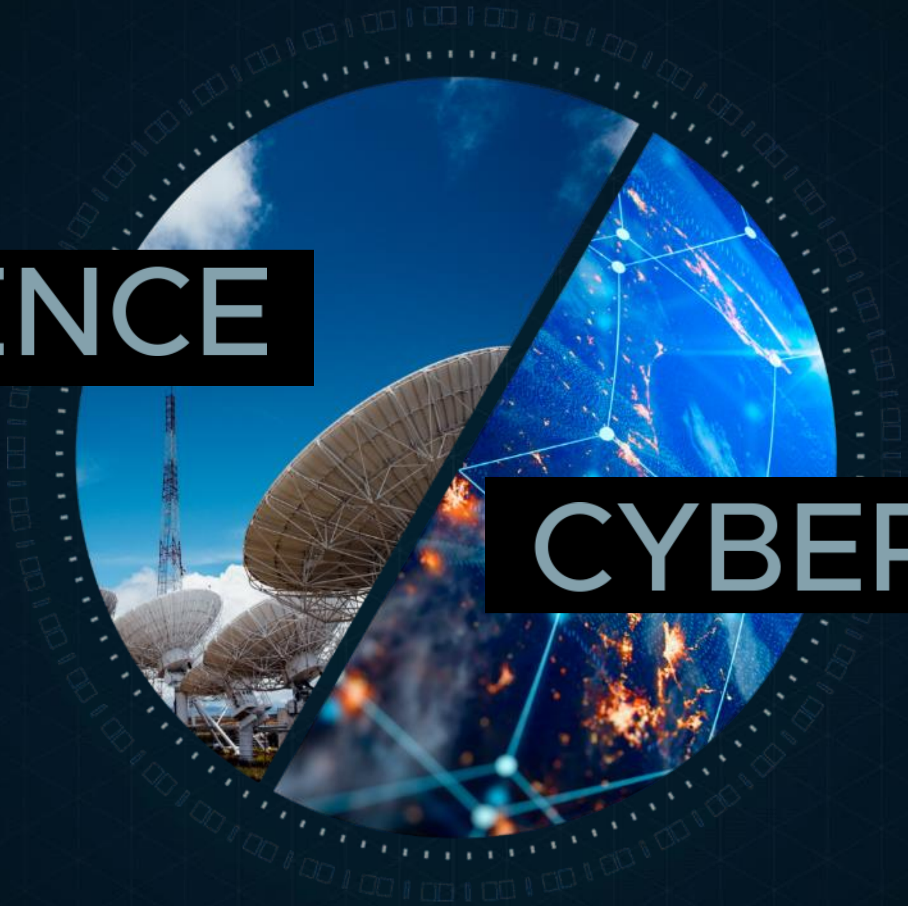
Published in NVD in 2022 – Less than

2% were exploited by malicious actors

Malicious actors **weaponize vulnerabilities** 40% faster than defenders remediate them and most organizations **remediate less than half of** known vulnerabilities.

What do you plan to do differently for vulnerability management by 2025? What are you doing now that needs bolstering?

THREAT-INFORMED DEFENSE



SIGNALS INTELLIGENCE

CYBERSECURITY

NSA's goal is to be the "signal through the noise" for the Defense Industrial Base

NSA Cybersecurity Collaboration Center

INFORMED BY NSA INTEL

UNCLASSIFIED ENGAGEMENTS

EMPOWERING “BEST-OF-BREED” COMPANIES

FREE CYBERSECURITY SERVICES FOR SMBs

Operationalizing Intelligence, Implementing the National Cybersecurity Strategy, and Protecting the DIB Ecosystem

Our Partners

400+ voluntary partners at every level of the DIB ecosystem.
All partnerships underpinned by an NDA, based on mutual benefit and trust

DIB PRIMES

DIB primes cover **80% of DoD acquisition spending**

DIB SERVICE PROVIDERS

IT and cybersecurity companies that **reach billions of endpoints**

DIB SMBs

DIB SMBs that support critical DoD programs

Our Cybersecurity Services

Designed to protect against the primary methods that adversaries are weaponizing against the DIB

Endorsed and Paid For by DoD CIO

Supports NIST 800-171 requirements

Provided through third parties (competitively awarded contracts)

Low barrier for entry: Active DoD contract (sub or prime) OR access to non-public DoD information

Bolstered by NSA threat intel

Our Core Services

& how they support NIST 800-171 controls

PROTECTIVE DNS (DNS FILTER)

NIST 800-171
System & Information Integrity
3.14.06

ATTACK SURFACE MANAGMENT

NIST 800-171
Risk Assessment
3.11.02, 3.11.03

THREAT INTELLIGENCE COLLABORATION

NIST 800-171
System & Information Integrity
3.14.03

Upcoming pilots include cloud security, threat hunting, phishing protection, and autonomous penetration testing

What does NSA get out of this?

- Secure warfighter (data, comms, weapons, etc.)
- Proprietary tech is protected, ensuring national security and economic advantage
- We understand how our adversaries are targeting the networks we care about the most (greater insights)
- We impact our adversaries’ cyber operations – with ripple effects
- We help SMBs below the “cyber poverty line”

What do you get out of this?

- Free stuff ☺
- Improved cyber hygiene
- Improved protection of your proprietary information
- Reduce risk of becoming a victim to a costly incident
- Support on your CMMC journey
- Access to additional cybersecurity pilots down the road

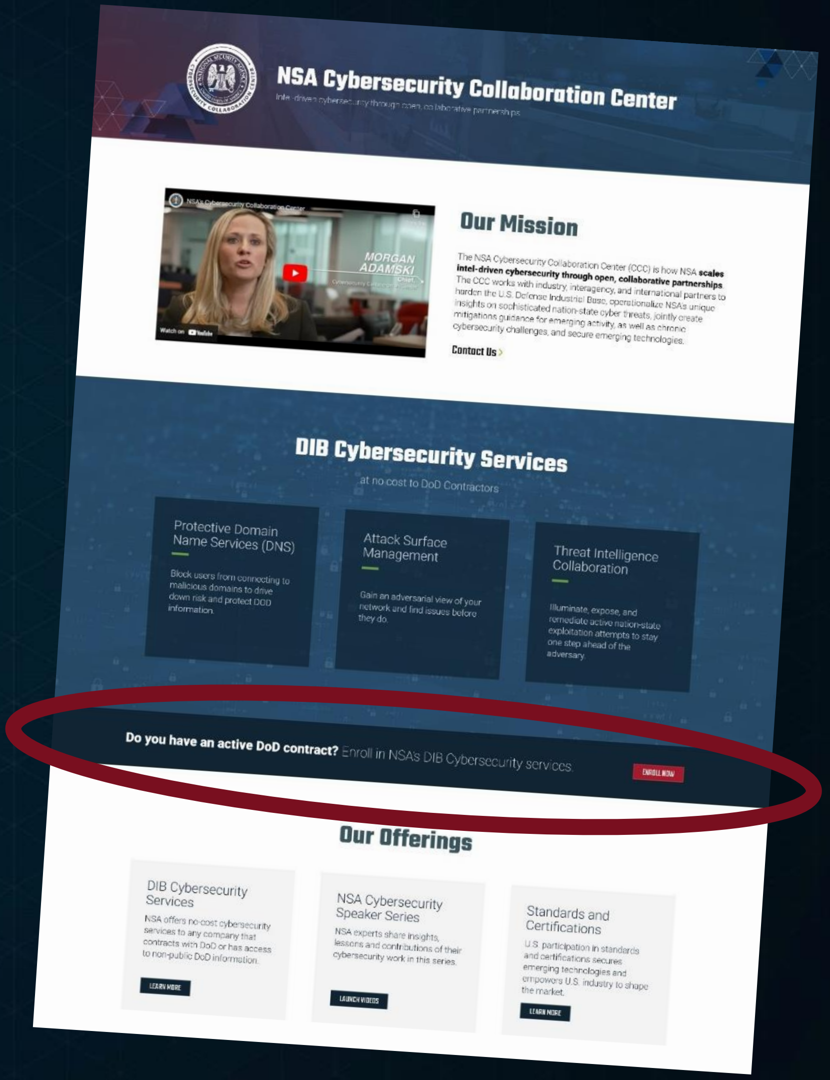
CALL TO ACTION: ENROLL & TELL YOUR FRIENDS

"Get Started"
www.nsa.gov/ccc

Eligibility
Confirmation

Sign
Agreement

Services
Enrollment



NSA Cybersecurity Collaboration Center

Intel-driven cybersecurity through open, collaborative partnerships

NSA's Cybersecurity Collaboration Center
MORGAN ADAMSKI
Chief,
Cybersecurity Collaboration Center
Watch on YouTube

Our Mission

The NSA Cybersecurity Collaboration Center (CCC) is how NSA **scales intel-driven cybersecurity through open, collaborative partnerships**. The CCC works with industry, interagency, and international partners to harden the U.S. Defense Industrial Base, operationalize NSA's unique insights on sophisticated nation-state cyber threats, jointly create mitigations guidance for emerging activity, as well as chronic cybersecurity challenges, and secure emerging technologies.

Contact Us >

DIB Cybersecurity Services

at no cost to DoD Contractors

Protective Domain Name Services (DNS)

Block users from connecting to malicious domains to drive down risk and protect DOD information.

Attack Surface Management

Gain an adversarial view of your network and find issues before they do.

Threat Intelligence Collaboration

Illuminate, expose, and remediate active nation-state exploitation attempts to stay one step ahead of the adversary.

Do you have an active DoD contract? Enroll in NSA's DIB Cybersecurity services.

Our Offerings

DIB Cybersecurity Services

NSA offers no-cost cybersecurity services to any company that contracts with DoD or has access to non-public DoD information.

NSA Cybersecurity Speaker Series

NSA experts share insights, lessons and contributions of their cybersecurity work in this series.

Standards and Certifications

U.S. participation in standards and certifications secures emerging technologies and empowers U.S. industry to shape the market.

In some cases, this process can take less than 15 minutes

DIB_DEFENSE@cyber.nsa.gov

www.NSA.gov/CCC

@NSAcyber