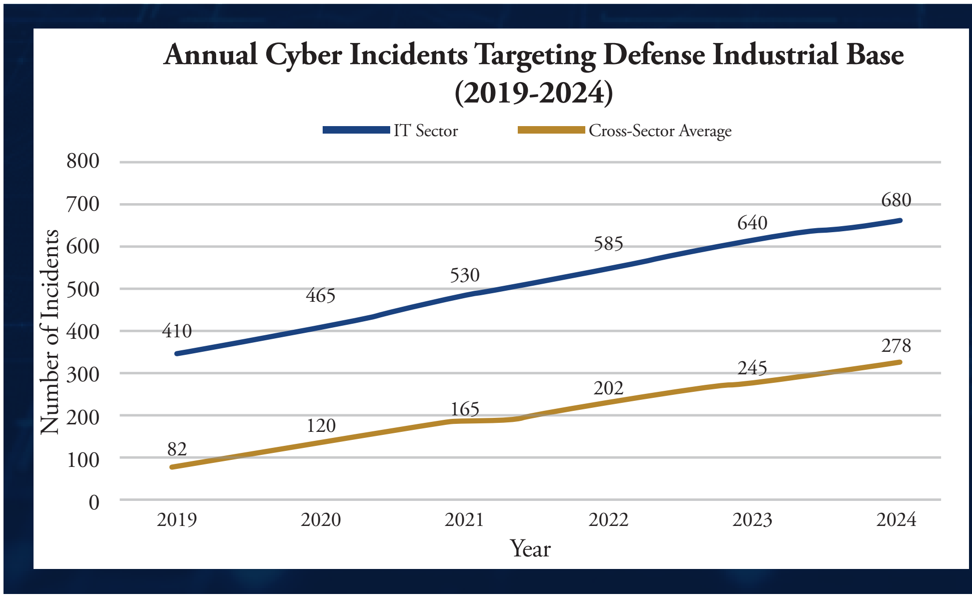
DEFENSE INDUSTRIAL BASE SECTOR CYBERSECURITY

Sector Overview

This resource is for stakeholders in Florida's Defense Industrial Base (DIB) sector. This includes Department of Defense contractors and subcontractors, weapons system manufacturers, aerospace and shipbuilding firms, cybersecurity integrators, and specialized technology suppliers. The DIB supports national defense readiness by delivering critical systems, components, and services to the U.S. military and allied forces. These organizations handle sensitive design data, military communications systems, and classified information. A ransomware incident could compromise national security, disrupt defense production schedules, and cause long-term loss of competitive advantage.

Ransomware Threat Profile

About 30% of Florida's DIB organizations meet the Department of Homeland Security's basic ransomware readiness standards, comparable to the Critical Manufacturing sector. The sector is a top target for both financially motivated cybercriminals and nation-state actors seeking to steal defense intellectual property (IP) or disrupt supply chains. Many DIB companies operate under strict cybersecurity compliance requirements such as NIST SP 800-171 and the Cybersecurity Maturity Model Certification (CMMC), but smaller subcontractors often struggle to meet these standards, creating exploitable weak links in the supply chain.



Note: Ransomware incidents in the Defense Industrial Base have more than doubled as a share of total Cyberattacks, rising from 20% in 2019 to 41% in 2024. Overall incidents climbed from 410 to 680 during this period, showing steady growth in targeting. This trend demonstrates ransomware as the DIB's top cyber threat.

Top Vulnerabilities

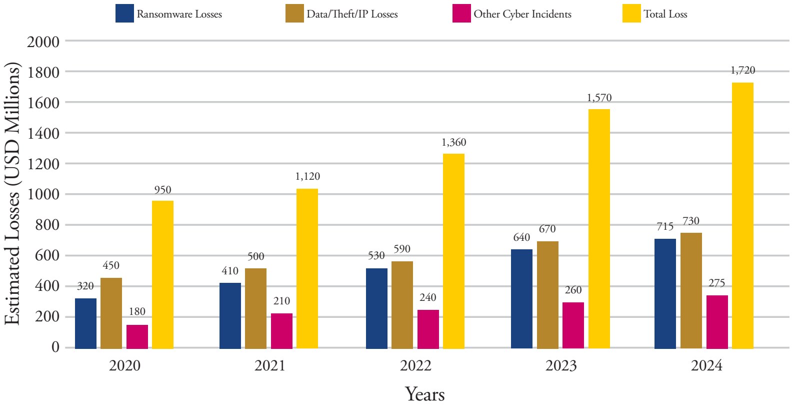
- **Defense Supply Chain Entry Points**
  - Nation-state actors often target smaller subcontractors with weaker defenses to pivot into prime contractor networks, ex-filtrating sensitive technical data.
- **Classified & Export-Controlled Data Exposure**
  - CAD files, weapons schematics, and controlled unclassified information (CUI) are high-value assets for ransomware gangs and espionage groups.
- **OT & Test System Integration Risks**
  - Defense manufacturing lines and testing facilities use OT/ICS environments linked to business networks, creating lateral movement paths for ransomware.
- **Vendor Remote Access & Maintenance Gaps**
  - Third-party maintenance teams for CNC machines, avionics test rigs, and production robots may lack MFA or continuous monitoring, offering covert access points.

DEFENSE INDUSTRIAL BASE SECTOR CYBERSECURITY

Action Checklist

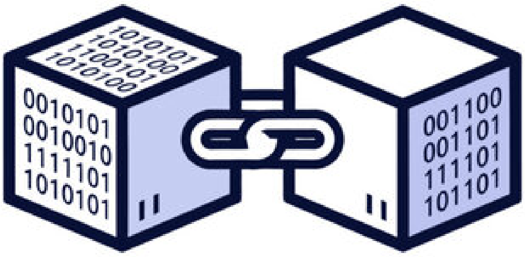
- ▶ Develop and test ransomware-specific Incident Response Plans that include classified and CUI handling procedures.
- ▶ Enforce MFA and privileged access monitoring across all classified, engineering, and production networks.
- ▶ Conduct annual ransomware tabletop exercises simulating supply chain breaches and operational disruptions.
- ▶ Audit and segment OT/ICS from business networks; enforce zero-trust policies for remote vendor access.
- ▶ Maintain encrypted, offline backups of design files, test data, and production schedules; verify restoration quarterly.
- ▶ Implement continuous network monitoring with anomaly detection tuned to detect espionage-related TTPs.
- ▶ Require supply chain partners to meet CMMC/NIST SP 800-171 security controls and document proof of compliance.

Estimated Annual Losses from Cyber Incidents in the DIB (2020-2024)



Notable Incidents

- ▶ **BAE Systems Supplier Breach (2024):** Ransomware hit a Tier-3 parts manufacturer, delaying shipment of aircraft components and forcing emergency sourcing.
- ▶ **LockBit Ransomware on Defense Subcontractor (2023):** A Florida-based subcontractor in the aerospace supply chain suffered a LockBit ransomware attack, resulting in encrypted engineering files and potential CUI compromise.
- ▶ **Aerojet Rocketdyne Breach (2022):** Cyberattackers accessed sensitive aerospace and missile propulsion design data, underscoring DIB vulnerability to advanced persistent threats.
- ▶ **Viasat Modem Disruption (2022):** A cyberattack disrupted satellite modems used for defense and intelligence communications, impacting U.S. and allied military operations.



Note: Annual cyber losses in the Defense Industrial Base grew from $950M in 2020 to $1.72B in 2024. Ransomware losses alone climbed from $320M to $715M, outpacing increases in data theft and other incidents. This makes it the sector's most costly threat.

State-Funded Resources & Education

Technical Tools

- **CISA Ransomware Readiness Assessment(CSET)**
- **Financial Services Information Sharing and Analysis Center (FS-ISAC)**

Templates & Planning

- **Cyber Florida Incident Response Plan Templates**
  Available Upon Request
- **NIST Cybersecurity Framework**
  (https://www.nist.gov/cyberframework)
- **FFIEC Cybersecurity Resource Center**

State-Funded Resources

- **FIU Cyber Leadership Courses**
  (https://gordoninstitute.fiu.edu/cybersecurity-policy/training/cybersecureflorida/index.html)
- **CISA Cyber Hygiene Services**
  Free Assessments & Scans
  (https://www.cisa.gov/resourcestools/ programs/cyberhygiene-services)