AN OFFERING IN THE BLUE CYBER SERIES:

DOD Cybersecurity Incident Reporting

Version 24 June 2021
#2 in the Blue Cyber Education Series

Small Business contracts contains many FARS and DFARS, some are listed some are referenced and you have to look them up. These are not all, but some key security requirements.

What is a DFARS? The Defense Federal Acquisition Regulation Supplement (DFARS) contains requirements of law, DoD-wide policies, delegations of FAR authorities, deviations from FAR requirements, and policies/procedures that have a significant effect on the public.

- **DFARS Clause 252.239-7010**: Cloud Computing Services
- **FAR Clause 252.204-21**: Basic Safeguarding of Covered Contractor Information Systems
- **DFARS Clause 252.204-7012**: Safeguarding Covered Defense Information and Cyber Incident Reporting
- **DFARS Clause 252.204-7008**: Compliance with safeguarding covered defense information controls
- **DFARS Clause 252.204-7020**: NIST SP 800-171 DoD Assessment Requirements.
- **DFARS Clause 252.204-7021**: Cybersecurity Maturity Model Certification Requirement
DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting

- Report cyber incidents
- Submit malicious software
- Facilitate damage assessment
- Safeguard covered defense information
What if there is a potential breach?

**Don’t panic.** Cybersecurity occurs in a dynamic environment. Hackers are constantly coming up with new ways to attack information systems, and DoD is constantly responding to these threats. Even if a contractor does everything right and institutes the strongest checks and controls, it is possible that someone will come up with a new way to penetrate these measures. DoD does not penalize contractors acting in good faith. The key is to work in partnership with DoD so that new strategies can be developed to stay one step ahead of the hackers.

**Contact DoD immediately.** Bad news does not get any better with time. These attacks threaten America’s national security and put service members’ lives at risk. DoD has to respond quickly to change operational plans and to implement measures to respond to new threats and vulnerabilities. Contractors should report any potential breaches to DoD **within 72 hours of discovery of any incident.**

**Be helpful and transparent.** Contractors must also cooperate with DoD to respond to security incidents. Contractors should immediately preserve and protect all evidence and capture as much information about the incident as possible. They should review their networks to identify compromised computers, services, data and user accounts and identify specific covered defense information that may have been lost or compromised.
What to Report to the Federal Government

DHS Definition: A cyber incident is an event that could jeopardize the confidentiality, integrity, or availability of digital information or information systems.

DFARS 7012 Definition: “Cyber incident” means actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein.

Report all cyber incidents that may:
- result in a significant loss of data, system availability, or control of systems;
- impact a large number of victims;
- indicate unauthorized access to, or malicious software present on, critical information technology systems;
- affect critical infrastructure or core government functions; or
- impact national security, economic security, or public health and safety.
Where to report cyber incidents/malware

To report cyber incidents that affect covered defense information or that affect the contractor’s ability to perform requirements designated as operationally critical support, the Contractor shall conduct a review for evidence of compromise and rapidly report cyber incidents to DoD at https://dibnet.dod.mil via an incident collection form (ICF).

If discovered and isolated in connection with a reported cyber incident, the contractor/ subcontractor shall submit the malicious software to the DoD Cyber Crime Center (DC3). Also, https://dibnet.dod.mil

If DoD elects to conduct a damage assessment, the Contracting Officer will be notified by the requiring activity to request media and damage assessment information from the contractor.
Welcome to the DIBNet portal
DoD's gateway for defense contractor reporting and voluntary participation in DoD's DIB Cybersecurity Program.

Cyber Reports

- Report a Cyber Incident

A Medium Assurance Certificate is required to report a Cyber Incident, applying to the DIB CS Program is not a prerequisite to report.

- DFARS 252-204-1012 Safeguarding Covered Defense Information and Cyber Incident Reporting
- DFARS 252-239-7010 Cloud Computing Services
- FAR 52.204-23 Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities
- FAR 52.204-25 Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment

Need Assistance?
Contact DoD Cyber Crime Center (DC3)
- DCISE@dc3.mil
- Hotline: (410) 981-0104
- Toll Free: (877) 838-2174

DoD's DIB Cybersecurity (CS) Program

- Apply Now

The DIB Program is a voluntary public-private cybersecurity partnership in which DoD and participants share threat information, mitigation and remediation strategies, and more.

- DIB CS Participant Login
- Voluntary Report

Cyber Threat Roundup
The Cyber Threat Roundup is a weekly collection of recent open-source articles of interest for the Defense Industrial Base. For the latest edition of the Cyber Threat Roundup, please click here.

Need Assistance?
Contact the DIB CS Program Office
- OUSD_DIBCSA@mail.mil
- Hotline: (703) 604-3167
- Toll Free: (855) DoD-IACS
- Fax: (571) 372-5434

A DoD-approved Medium Assurance Certificate is required to access DIBNet services. To obtain a DoD-approved Medium Assurance Certificate, please click here.

Cyber Threat Roundup

A collection of recent open-source items of interest to the Defense Industrial Base

Contents

Articles

REvil Ransomware Hits US Nuclear Weapons Contractor ......................................................... 2
G7 Leaders Ask Russia to Hunt Down Ransomware Gangs Within its Borders .......................... 2
Microsoft: SEO Poisoning Used to Backdoor Targets with Malware .................................. 2
Wear your MASQ! New Device Fingerprint Spoofing Tool Available in Dark Web .................. 3
Hackers Can Exploit Samsung Pre-Installed Apps to Spy On Users .................................... 3
New Cyber Espionage Group Targeting Ministries of Foreign Affairs .................................. 3
Experts Shed Light On Distinctive Tactics Used by Hades Ransomware ............................. 4
Paradise Ransomware Source Code Released on a Hacking Forum .................................. 4
Microsoft: Scammers Bypass Office 365 MFA in BEC Attacks ............................................ 5
Researchers Uncover ‘Process Ghosting’ — A New Malware Evasion Technique ................. 5
DCISE Overview

DoD Defense Industrial Base Collaborative Information Sharing Environment (DCISE)—DCISE is the operational hub of DoD's Defense Industrial Base (DIB) Cybersecurity Program, focused on protecting intellectual property and safeguarding DoD content residing on or transmitted through contractor unclassified networks. The public-private cybersecurity partnership provides a collaborative environment to share known threats and threat intelligence across unclassified networks.

DoD DCISE is the reporting and analysis hub for implementation of Section 941 of the Fiscal Year 2013 National Defense Authorization Act regarding certain types of cyber incidents by cleared defense contractors (CDCs) and the related Defense Federal Acquisition Regulation Supplement (DFARS 252.204-7012). Cyber incidents outlined in the DFARS are submitted to DC3/DCISE as mandatory reports; however, all other cyber events can be reported voluntarily.

- Rated as Capability Maturity Model Integration for Services (CMMI-SVC) Maturity Level 3
- Collaborative partnership with over 85,000 CDCs and U.S. Government (USG) agencies
- Shared over 450,000 actionable, non-attributable (to submitting source) indicators
- Provided over 77,000 hours of no-cost forensics and malware analysis for DIB Partners
- Disseminated 12,500+ cyber threat reports for both DIB and USG consumption (DIB partners may access DCISE reporting via their DIBNET accounts and USG members can access via SPIR Interactive)
- Operates 24/7/365 DCISE support hotline to assist subcontractors and DIB & USG Partners

DCISE Fact Sheet  DCISE Stick Sheets  DCISE News

Contact Us

Phone: 410-981-0104
Toll Free: 1.877.838.2174
Email: DCISE@dc3.mil

DCISE

Click to subscribe and receive future communications and updates

DIBNET PORTAL

DoD's gateway for defense contractor reporting and voluntary participation in DoDx's DIB Cybersecurity Program.

DIB Cyber Reports  DIB CS Program
DC3 CAPABILITIES FOR DoD REQUIREMENTS

FORENSIC LAB SERVICES
DoC Center of Excellence for Digital and Multimedia (D/MM) forensics, DC3 Cyber Forensics Lab is an ISO 17025 accredited lab that performs D/MM forensic examinations, device repair, data extraction, and expert testimony for DoD.
- Network Intrusions
- Malware/Reverse Engineering
- Enhancing Video and Voice Recordings
- Aircraft Mishap Data Recovery
- Damaged Media and Submerged Devices
- Mobile Device Encryption/Recovery
- DOMEX Forensic Partner

MISSION STATEMENT
Deliver superior digital and multimedia (D/MM) forensic services, cyber technical training, vulnerability sharing, technical solutions development, and cyber analysis within the following DoD mission areas: cybersecurity and critical infrastructure protection, law enforcement and counterintelligence, document and media exploitation, and counterterrorism.

VISION STATEMENT
Digital and multimedia technical and analytical center of excellence to improve DoD mission assurance and enhance warfighter capability.

DEFENSE INDUSTRY SHARING
DoD focal point for all cyberincident reporting affecting unclassified networks of Defense Industrial Base (DIB) contractors.
- Cyber Threat Information Sharing with DIB
- Cyber Incident and Malware Analysis
- Pilot Service Offerings (CSaaS)
- Mitigation and Remediation Strategies
- Partnership Exchanges
- Cyber Resiliency Analyses

VULNERABILITY MANAGEMENT
DoD Vulnerability Disclosure Program Lead. Includes collaborative efforts with private-sector cybersecurity researchers to crowdsource the identification of vulnerabilities on DoD networks and systems.
- Enhance Security of DoD Networks/Systems
- Independent Assessment of Cyber Defenses
- Improve Mission Assurance

OPERATIONS ENABLEMENT
Amplifies the collective effects of DoD-wide law enforcement and counterintelligence investigations and operations by conducting expert technical analysis and all-source analysis and developing enhanced operational support capabilities.
- Collaborative Analytics with LE/CIV/IC
- Focused All Source Intelligence
- Tailored Operational Production
- StormSystem Enhancement and Deployment
- CADO-IS Development and Integration

CYBER TRAINING
Provides specialized in-residence and online cyber training (www.dctca.edu).
- Cyber Protection Team Training
- Network Defense
- Computer Technologies
- Basic and Advanced Forensic Examination
- Distance Learning/Webinar/Mobile Training
- Digital Forensics Certifications

TECHNICAL SOLUTIONS
Tailored software and system solutions to support digital forensic examiners, DOMEX, and cyber intrusion analysis.
- Tool and Software Development
- Tool Test/Validation (Including GOTS/COTS)
- Counterintelligence Tool Repository
- Automated Malware Processing
Any Questions?

• This briefing is not a substitute for reading the FARS/DFARS

• Resources and more modules like this are coming every day!

• Please provide questions, feedback or if you just want to talk about your cyber security /data protection questions to: Kelley.Kiernan@us.af.mil
  - Office hours daily for answering/researching your DAF Small Business questions!