CURRENT DOD DIB CYBERSECURITY EFFORTS

CYBER THREAT INFORMATION/ INTELLIGENCE SHARING WITH DIB

- **DoD CISO/DIB CS Program –** voluntary public-private cybersecurity partnership between DoD and DIB to share information/intelligence; manages intel sharing platform, hosts events, maintains comms, and enables info/intel sharing
- **DC3/DCISE –** operational arm of DIB CS Program, sharing cyber threat info/intelligence, products, and tools to assist DIB
- **NSA –** shares "left of boom" products and tools with DIB

INCIDENT REPORTING

- **DoD CISO/DIB CS Program –** Oversight of DFARS 252.204-7012*; management of platform for voluntary and mandatory reporting; enables efforts to assess damage to DoD programs
- **DC3/DCISE –** single clearinghouse for unclassified Mandatory Incident Reports (MIR) per DFARS -7012; provides crowd-sourced, non-attributional reports to DIB on cyber threat information received from MIRs and voluntary reports
- **DCSA –** single clearinghouse for classified incident reports

DFARS 252.204-7012 ("DFARS-7012") stipulates a contractor's requirement to rapidly report cyber incidents within 72 hours of discovery at https://dibnet.dod.mil (DIBNet) and protect CUI.

DIB CYBERSECURITY REQUIREMENTS & ASSESSMENT MECHANISMS

- **DoD CISO/DIB CS Program –** assistance to DIB in understanding regulatory requirements
- **DCMA –** Oversight of DFARS 252.204-7019/7020*, DIBCAC
- **USD(A&S) –** Oversight of DFARS 252.204-7021*, CMMC

DFARS 252.204-7019/7020 stipulates a contractor's requirement to implement NIST SP 800-171, have an assessment (basic, medium, or high), and prove ability to protect CUI.

DFARS 252.204-7021 stipulates a contractor have current CMMC certificate at the CMMC level required by the contract, and maintain the certificate at the required level for the duration of the contract.

CYBERSECURITY TECHNICAL ASSISTANCE AND COLLABORATION

- **DoD CISO/DIB CS Program –** offers vehicle for DoD collaboration with DIB, establishing and or maintaining relationships; hosts events, sub-working groups, and forums for collaboration
- **DC3/DCISE –** direct support to DIB through cost-free service offerings including: products, tools, strategies, and events
- **NSA –** targeted support to top-tier DIB for companies categorized as critical infrastructure

Additional official DoD policy/guidance is required to clearly assign all DIB roles and responsibilities

1