INCIDENT INFORMATION TO REPORT

The Department of Defense (DoD) contractor shall report as much of the following information to DoD within 72 hours of discovery of a cyber incident:

1. Company name
2. Company point of contact information (address, position, telephone, email)
3. Data Universal Numbering System (DUNS) Number
4. Contract number(s) or other type of agreement affected or potentially affected
5. Contracting Officer or other type of agreement point of contact (address, position, telephone, email)
6. USG Program Manager point of contact (address, position, telephone, email)
7. Contract or other type of agreement clearance level (Unclassified, Confidential, Secret, Top Secret, Not applicable)
8. Facility CAGE code
9. Facility Clearance Level (Unclassified, Confidential, Secret, Top Secret, Not applicable)
10. Impact to Covered Defense Information
11. Ability to provide operationally critical support
12. Date incident discovered
13. Location(s) of compromise
14. Incident location CAGE code
15. DoD programs, platforms or systems involved
16. Type of compromise (unauthorized access, unauthorized release (includes inadvertent release), unknown, not applicable)
17. Description of technique or method used in cyber incident
18. Incident outcome (successful compromise, failed attempt, unknown)
19. Incident/Compromise narrative
20. Any additional information

When reporting a cyber incident, the contractor will access the DIBNet portal, https://dibnet.dod.mil/portal/intranet, and complete the above in the Incident Collection Format (ICF).

CROSS TIMBERS

Procurement Technical Assistance Center

Medium Assurance Public Key Infrastructure (PKI) Certificate

Access to the DibNet ICF, you must have a DoD approved medium assurance Public Key Infrastructure (PKI) certificate:

- The Separate Security Certificate is issued to the individuals, not a company, needed to communicate with DoD resources
- You must gain approval from one of these two approved vendors
    - WidePoint
    - IdenTrust
- Approval / validation process to obtain PKI
- Can take up to 45 days to obtain
- Begin the certification process here: https://public.cyber.mil/eca/

CROSS TIMBERS
Procurement Technical Assistance Center