



DEPARTMENT OF THE AIR FORCE
WASHINGTON, DC

OFFICE OF THE SECRETARY

10 September 2020

MEMORANDUM FOR DEPARTMENT OF THE AIR FORCE (DAF) SMALL BUSINESSES

FROM: DAF Chief Information Security Officer

SUBJECT: Cyber Security and Resiliency Information for Small Businesses

References: Attached

1. Understanding and managing risk for all Information Technology (IT) is of paramount importance. The intent of this memo is to provide information to help Small Businesses frame their Cybersecurity approach. Attached are references to provide additional details and this information allows you to outline your efforts to address cybersecurity:

- a. To operate in the Department of the Air Force (DAF) every IT must obtain an Authority to Operate using the Risk Management Framework (RMF) assessment. To achieve cybersecurity objectives the DAF project manager/sponsor for a system in development should consult with the applicable cybersecurity office.
- b. The DoD has published a number of Security Technical Implementation Guidelines and Security Requirements Guidelines to ensure systems address key requirements. In addition, fundamental cybersecurity control measures are outlined in NIST SP 800-171 Revision 1 and DFAR PGI 239.76-Cloud Computing.
- c. All acquisitions of systems containing IT must have a Cybersecurity Strategy (CSS). The CSS is a required acquisition document that details how a program will ensure the IT can protect and defend itself from a cyber-attack.
- d. The DAF is migrating to the cloud and have aligned software development efforts towards Cloud One, Platform One and the use of software factories. It is important to establish your DevSecOps in a secure Cloud environment that meets your business needs.
- e. Fundamental cybersecurity areas for consideration also include information and data protections actions for Controlled Unclassified Information to include PII, PHI, and other data categories. Data must be protected at the appropriate level.
- f. Another measure of cybersecurity and preparation is the ability for industry partners to meet the Cybersecurity Maturity Model Certification requirements.

2. These focus areas will set you on the path to meet the cybersecurity and resiliency objectives of the DAF. There is a Cybersecurity and Information Security slide deck and Frequently Asked Questions located on www.afsbirsttr.af.mil to guide you and your DAF program to create a holistic briefing on your IT system. If you still have questions, ask them via the Air Force SBIR/STTR Help Desk at usaf.team@afsbirsttr.us.

WANDA JONES-HEATH, SES, DAF
DAF Chief Information Security Officer

Attachment: References

REFERENCES

- (a) NIST SP 800-37 Rev 2, 20 December 2018, *Risk Management Framework (RMF) for Information Systems and Organizations* <https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final>
- (b) NIST SP 800-171 Rev 2, 21 February 2020, *Protecting Controlled Unclassified Information (CUI) in Nonfederal Systems and Organizations* <https://csrc.nist.gov/news/2020/nist-publishes-sp-800-171-rev-2-protecting-cui>
- (c) DFAR PGI 239.76-CLOUD COMPUTING
https://www.acq.osd.mil/dpap/dars/dfars/html/current/239_76.htm#BM239_76
- (d) DoDI 5000.82, 21 April 2020, *Acquisition of Information Technology*
<https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500082p.pdf>
- (e) DoDI 8510.01, Change 2, 28 July 2017, *Risk Management Framework (RMF) for DoD Information Technology*
<https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/851001p.pdf?ver=2019-02-26-101520-300>
- (f) DoDI 8580.1, 9 July 2004, *Information Assurance (IA) in the Defense Acquisition System*
<https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/858001p.pdf>
- (g) AFI 17-101, 6 February 2020, *Risk Management Framework (RMF) for Air Force Information Technology (IT)*
https://static.e-publishing.af.mil/production/1/saf_cn/publication/afi17-101/afi17-101.pdf
- (h) AFI 17-130, 13 February 2020, *Cybersecurity Program Management* https://static.e-publishing.af.mil/production/1/saf_cn/publication/afi17-130/afi17-130.pdf
- (i) Assistant Secretary of Acquisition, Chief Software Office, <https://software.af.mil/>
- (j) Office of the Under Secretary of Defense for Acquisition & Sustainment Cybersecurity Maturity Model Certification, <https://www.acq.osd.mil/cmmc/index.html>