Workplace 3.0
Attachment 7: Minimum Cybersecurity Requirements

Solicitation Number: HT0038-21-S-CS003
Program Executive Office, Healthcare Management Systems (PEO DHMS)

SECTION I

1.0 Purpose

The purpose of Attachment 7 is to provide awareness to Applicants of the minimum set of cybersecurity requirements for technical solutions as they proceed through the Workplace 3.0 (WP3) Commercial Solutions Opening (CSO) process. For a future partner to provide technical solutions to the Government, and particularly the PEO DHMS and its stakeholders, there needs to be a mutual understanding of these requirements, and they will be a key component of evaluation through each phase of the CSO. While it is not expected for proof of all requirements to be demonstrated through the Abstract-Pitch-Proposal Phases, there should be acknowledgement and understanding that these requirements will be met for technical solutions when it comes time to execute.

2.0 Background

Similar to many Government organizations, especially those within the Defense and Health space, PEO DHMS prioritizes the protection and security of data and information handled on a daily basis. Our organization and the systems we utilize routinely manage sensitive data, such as Controlled Unclassified Information (CUI), Personally Identifiable Information (PII), and Protected Health Information (PHI). We must be deliberate about adhering to the policies and regulations mandated by the government to maintain the trust in our organization and security of our systems. We see technology being an integral part of the WP3, and therefore must ensure we are diligent about introducing technical solutions and applicable manpower in a manner that maintains the expected high level of integrity.

3.0 Minimum Cybersecurity Requirements

The level of involvement for regulations and requirements will depend on the services and capabilities proposed as part of a solution. In order for an organization to meet the minimum cybersecurity standard, there should be a fundamental understanding of the following set of regulations, which can be broken down into technical requirements and manpower requirements.

- Technical
    - NIST Special Publication 800-171 revision 2
      https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf
    - NIST Special Publication 800-37 revision 2
      https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final
    - NIST Special Publication 800-53 Revision 5
      https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
    - DFAR 252.204-7020 and 252.204-7021
      https://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm#252.204-7020
      https://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm#252.204-7021
    - FedRAMP – Cloud services involving Controlled Unclassified information (CUI), PII and PHI will require an Impact Level 4 (IL4) minimum
    - https://www.acq.osd.mil/cmmc/
    - *https://www.fedramp.gov/*

As a guide, please see NIST Handbook 163 for help with a self-assessment.

- IT/IA Workforce

- DoD Directive 8140.01
  https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/814001p.pdf
- DoD 8570.01-M (specifically, the Role and Responsibility Compliance Matrix)
  https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/857001m.pdf
- *https://public.cyber.mil/cw/cwmp/dod-approved-8570-baseline-certifications/*

The fundamental understanding of these requirements is mandatory to operate in the DoD space. Additional, more granular, requirements may be imposed based on the type of solution being presented. This will take place as we proceed into the late phases of the CSO process where technical reviews of the solution may occur. Any misrepresentation of the partners capabilities will have repercussions that may include a Stop Work Order or a cancellation of a contract for cause.

While these requirements are more stringent than what is typical in the commercial space, we intend to work closely with organizations to navigate regulations and manage risk together as we introduce innovation into our workplace.