Tuesday Tips is a new outreach effort by OGCA. The idea behind *Tuesday Tips* is to convey tips, tricks and other helpful information around the area of research administration. Our goal is to post on (almost every) Tuesdays. If there is something you would like to see covered on *Tuesday Tips*, email: UAF-GCReATE@alaska.edu. For more Tips visit OGCA website.

Cybersecurity Maturity Model Certification (CMMC)

Federal Government and Department of Defense related research contracts with the DFARS 252.204-7012 clause.pdf and Export Control (ITAR/EAR), have required compliance with the Cybersecurity Capability Maturity Model (CMMC) Level 3 that includes the NIST SP 800-171.pdf security controls to safeguard Controlled Unclassified Information (CUI). CUI is data that requires protection through dissemination controls pursuant to and consistent with applicable law, regulations and government-wide policies but is not classified.

CMMC applies to CUI shared by or through the federal government with a nonfederal entity. As a higher educational institution, UAF is a non-federal entity. There are 130 technical and operational controls specified by the CMMC/NIST standard and ITS has made every effort to reduce the compliance efforts for the Principal Investigator (PI).

The Secured Research Infrastructure (SRI) was developed with the intent of meeting the security control requirements while also reducing the workload

on the PI to the smallest amount practical while still ensuring compliance. This solution meets 3 key design principles:

- The controls requirements established by the CMMC/NIST standard are complex. Each research project will be reviewed for its specific technical requirements to properly safeguard CUI. Ensuring controls consistency reduces the time to bring a new project into the environment and increases the ability to ensure compliance.

- The system needs to provide the ability for researchers, whenever practical, to access and work with their data anywhere and have the environment be supported centrally.

- The security controls should be provided centrally. University of Alaska Records and Information Management has made significant investments in our enterprise level security infrastructure and operational processes that enable us to protect CUI using centrally supported tools with more capabilities that can be provided locally.

Beginning November 30, 2020, DoD will incorporate requirements for CMMC into selected Requests for Proposals (RFPs), Requests for Information (RFIs), and research contracts. By October 1, 2025, all DoD contract awards will require CMMC certification to Level 1 at a minimum. CMMC requirements will not be applied retroactively to existing contracts.

The Office of Grants and Contracts Administration has addition information and updates on CMMC.