ITPS - CMMC Webinar
8/14/20
Host and Presenter: Robert Smith, Systemwide IT Policy
Co-Presenters: Mike Cullen and Matt Gilbert – Baker Tilly

10:06:35 From Ezra Van Everbroeck : CMMC = “Cybersecurity Maturity Model Certification”

10:06:50 From Ezra Van Everbroeck : (https://www.acq.osd.mil/cmmc/)

10:09:01 From Mike Cullen: Here is the CMMC AB website, they are administrating the program. https://www.cmmcab.org/

10:09:31 From Matt Gilbert : The certification lasts 3 years so long as no major changes or major breach occurs

10:09:54 From Anthony Drown : Do we have a link to the controls?

10:09:59 From Anthony Drown : v1.02

10:10:21 From Mike Cullen : Model w controls = https://www.acq.osd.mil/cmmc/draft.html

10:12:24 From noampines : If orgs get certified over 5 year period, what is compliance risk if "not ready" by 2021 (but not selected until later)?

10:13:39 From Matt Gilbert : this only applies to future awards so as long as you are certified before award you are fine. But the risk is lack of complete clarity when and which awards will have the requirement

10:13:57 From noampines : I recall a possibility that some cert would be necessary with proposal submissions. Is that still in play?

10:14:05 From Brittany Whiting : This can come in on contract amendments possibly too

10:14:10 From noampines : Ah, thanks Matt. That makes sense.

10:14:43 From noampines : Yikes - do we know that for sure re: amendments?

10:16:05 From Matt Gilbert : Yes we intend to be CA and Baker Tilly intends to be a C3PAO. I am also on the working groups helping the CMMC-AB currently.

10:17:09 From Matt Gilbert : The question about contract mods we should touch on later in the Q&A because it is a longer answer. Don't let us forget to hit that one.

10:18:05 From Dewight F Kramer : Yes Zoom stated it is being recorded

10:18:16 From Brittany Whiting : clarifications not amendments, but new contracts that would be follow on to awards.

10:21:04 From KENTON LEFORE : is the CMMC certification for an entire campus or is for an individual academic department, or for a specific PI's research unit?

10:26:10 From Matt Gilbert : How you choose to scope is going to be critical. You might want to have a level 1 cert for grants administration because they will have FCI but not CUI and then you establish a lab as level 3 because you will keep all the CUI in the lab only. This will allow you to keep cost and protections aligned to the associated data.

10:28:04 From Mike Cullen : Note that CMMC has 17 domains, NIST SP 800-171 only has 14. So the three additional domains are: Asset Management (AM), Recovery (RE), and Situational Awareness (SA).

10:28:22 From Quico Gonzalez : Hi Matt, would we be able to get certified in a lab at Level 3 w/o the unit achieving level 1 cert?

10:28:44 From Jamie Lam : How do you budget for the certification process when it's done at the lab level?

10:29:12 From Kenneth Newton : Would that mean members of UC have access to DIBNET?

10:30:44 From Dewight F Kramer : Does this mean that this CMMC would not impact Grants?

10:30:52 From Matt Gilbert : Yes you could have a lab at level 3 and other areas wouldn't need to be certified but only if they never have FCI or CUI. Effectively the data should define / align to the cert

10:31:29 From Mike Cullen : To achieve certification you will have to define the boundary very specifically. So you could have a lab certified at level 3 but the department could be a different level. However, that would require some very specific scoping so folks are clear on the boundary protecting the data.

10:31:42 From noampines : Do you have to certify at a certain level, just for the possibility that researchers may have to handle CUI from the gov't? (ed institution)

10:32:02 From Natalie Tedford : Are the contracts referenced here direct federal contracts alone, or does it include federal flow through subcontracts?

10:32:26 From Mike Cullen : CMMC applies to subcontracts as well.

10:32:55 From Mike Cullen : CMMC will likely apply to grants. However, how that might work will depend on the official rulemaking.

10:32:56 From Natalie Tedford : Just wondering what the table includes -- amounts seem low.

10:33:26 From Mike Cullen : DoD has said that is you have CUI you need to be Level 3.

10:35:27 From Mike Cullen : Budgeting for the costs of certification will depend on the boundary of what you get certified. If you do it at the individual lab level that could get costly very quickly. Another method could be to create a certified enclave and have multiple labs/departments use that certified enclave.

10:36:22 From Ezra Van Everbroeck : If you have DoD CUI, you should already be NIST 800-171 compliant. There is a self-assessment guide as well, and DoD will be asking contractors to submit their self-assessment score into their database. This is separate from CMMC.

10:36:27 From Mike Cullen : DFARS website = https://www.acq.osd.mil/dpap/dars/dfarspgi/current/index.html

10:37:21 From Matt Gilbert : That is correct. Historically, 800-171 would allow POA&Ms and CMMC will not.

10:38:24 From Matt Gilbert : so between no ability to have POA&Ms and an external inspection not just self cert. the bar is increasing.

10:38:36 From noampines : POA&Ms?

10:38:53 From Rainier Elias (OGC) : Plan of Action/Mitigations

10:38:55 From Jamie Lam : Is it accurate to say that every campus will need at least a level 1 certification for their grants administration office?

10:38:56 From Matt Gilbert : Sorry Plan of Actions and Milestones

10:39:10 From Rainier Elias (OGC) : or milestones

10:39:14 From noampines : Thanks!

10:39:37 From Mike Cullen : POAM (NIST def) = https://csrc.nist.gov/glossary/term/POAM

10:40:28 From Mike Cullen : NIST 800-53 control for POA&Ms = https://nvd.nist.gov/800-53/Rev4/control/PM-4

10:41:14 From Matt Gilbert : If you have a DoD contract and plan to continue to have DoD contracts then that is FCI. If you have FCI you are going to need to be level 1. If no FCI or DoD contracts then no need for level 1.

10:42:17 From Dewight F Kramer : When yo say get on track, it will be based on the research, as the campus no longer is required to be level 1

10:42:31 From noampines : Yeah, level 1 vs level 3 for universities is unclear. Sorry to go down the wormhole, but our current stance is we can't produce CUI because of the risk for FRE. But we can handle it from the gov't (in theory). I don't think we've had to do that, but one question is - do we have to do level 3 just in case?

10:42:35 From Dewight F Kramer : So what is meant to get on track?

10:43:23 From noampines : Sounds like specific "enclave" is the answer?

10:44:11 From Dewight F Kramer : Has UCOP Procurement started looking at identifying companies that we can use to certify?

10:46:07 From Mike Cullen : If you receive CUI from DoD you will need to be Level 3, under current guidance.

10:46:08 From Matt Gilbert : Without your specific circumstances in mind it is hard to say the answer but on the whole I would suggest smart use of enclaves is a good option.

10:46:11 From Steve Pigg : How is this different than DOD planning to require NIST 800-171 back in 2016? Do we believe they will follow through now when they did not in the past?

10:47:45 From Mike Cullen : Prior requirements for NIST 800-171 did not have an external certification process, CMMC does. And now there is an entire organization CMMC AB that has been stood up to administer the certifications.

10:49:16 From Matt Gilbert : Without an ability to tell the future it is hard to say for certain. Laws could be written to shield universities. But in the absence the big difference is the need to be assessed by a 3rd party to get the certification. Under 800-171 even if it made it into the contract it would be easy to represent that you are fine without 3rd party verification.

10:51:24 From Ezra Van Everbroeck : If anyone is interested in what the DoD is telling its own contracting officers about CMMC, here's a webinar from earlier this week:

10:51:26 From Ezra Van Everbroeck : https://www.dau.edu/events/DAU%20Webcasts%20-%20The%20Cybersecurity%20Maturity%20Model%20Certification%20-%20Latest%20Developments

10:52:26 From Quico Gonzalez : Are there any success stories or suggestions on how to change the culture that will be required for researchers to begin working with security, IT, and other external units to meet these requirements where before they were accustomed to be self sufficient due to the self reporting limitations?

10:54:45 From Dewight F Kramer : Does that mean that 3rd parties need to have CMMC Cert too like PCI?

10:54:53 From Dewight F Kramer : You know AWS M.S.

10:55:17 From Steve Pigg : If you want researchers to pay attention, locations will need to implement processes that inform and hold PIs accountable at the proposal step.

10:55:39 From Mike Cullen : If the 3rd party has access to FCI or CUI they will have to be certified.

10:56:16 From Dewight F Kramer : So is MS, AWS, Google…. Getting this certification?

10:56:53 From KENTON LEFORE : If a portion of a research lab's computing function is provided by a central campus IT unit, does the central IT unit also need to be certified?

10:57:35 From Joe Schiffman : Isn't that Govcloud instances only? EDU is on different instances.

10:58:51 From Dewight F Kramer : How does that time constraint work with researchers?

10:59:38 From Dewight F Kramer : If we are limiting or scoping this to researchers then really there needs to be an standing environment

11:02:10 From Dewight F Kramer : Can UCOP or the UC become or develop offices for C3PAO

11:02:47 From Dewight F Kramer : So that we can be more flexible in getting researchers certified in the very time crunched requirements

11:03:27 From dcassada : I don't think that would work, would have to be independent.

11:04:59 From Dewight F Kramer : If you are focusing on the scope of the researcher based on the slide earlier you are looking at 900-1200+ certifications that all need to be done very quickly to stay competitive

11:05:30 From Dewight F Kramer : Or it is not really scoped on researchers you just have an environment that is and force researchers into it

11:05:36 From Dewight F Kramer : Which does not work well

11:06:09 From John Denune : But compliance has to scale somehow… It will be a challenge either way.

11:06:37 From dcassada : Standard set of controls everyone adopts doesn't have to be the same exact tools.

11:08:23 From dcassada : Writing a research computing standard may be the way to go w/ optional secure multi-tenant environment.

11:10:40 From Dewight F Kramer : Then it is not scoped to the researcher, it is scoped to the environment and it is very hard to get Faculty to move that way

11:10:45 From Dewight F Kramer : Thank you for the answer though

11:12:21 From Dewight F Kramer : Yes PCI is a good example but it is a very different type of engagement

11:12:57 From dcassada : Generic controls (full disk encryption, multi factor authentication, roles for access provisioning to assign, etc) or use this multi-tenant environments at cost w/ shared services.

11:13:37 From Mike Cullen : Dewight, you are correct getting faculty to move that way is difficult. We have had success showing faculty the value of these more "centralized/shared" tools to protecting the integrity of their research and therefore their professional reputations.

11:15:19 From Steve Pigg : When it comes down to it, if an enclave is certified, the researchers may have little choice but to select something that allows them to do their research quickly.