POST AWARD MODIFICATIONS QUESTIONS

1. For projects in construction, is there Independent Government Estimate (IGE) guidance for modifications?

   No IGE guidance is provided for modifications but it is expected to be minimal since UFGS 25 50 00.00 20 is not requiring additional hardware/software, only configuration and documentation for products already being provided. The preference is to include UFGS 25 50 00.00 20 in the pre-award documents in lieu of post-award modifications in order to minimize the impact to cost and schedule.

2. For projects in construction, is there guidance for how to negotiate modifications? If we cannot negotiate a modification within IGE/guidance, do we still award the modification? Is there a point where this might not be worth it?

   No modification negotiation guidance is provided but if the project teams are receiving proposals that are unreasonable for the configuration and documentation for products already being provided, then it stands to reason to not award. But it will be important to ensure the Contractor understands the true nature of the modification. In order to circumvent this situation, it would be prudent to discuss the details of UFGS 25 50 00.00 20 with the Contractor to ensure they understand the requirements prior to issuing the modification.

3. Is CIO4 going to support negotiations of a modification, when it comes to clarifying for the Contractor how much effort is expected?

   Modification negotiation guidance will not be coming from CIO4 but if the project teams are receiving proposals that are unreasonable for the configuration and documentation for products already being provided, then it stands to reason to not award. But it will be important to ensure the Contractor understands the true nature of the modification; it would be prudent to discuss the details of UFGS 25 50 00.00 20 with the Contractor to ensure they understand the requirements prior to issuing the modification.

4. Who is the lead for the "Cybersecurity of Control Systems" at the Pre-Construction Meeting, CIO4?

   The Construction Manager (CM) is the lead for the Pre-Construction Meeting and should highlight that there is a requirement to submit information about the project control systems for the "Cybersecurity of Control Systems" topic. CIO4 should be invited and assist with the cybersecurity discussion only to highlight the specification requirements of UFGS 25 50 00.00 20. The CM needs to ensure that no additional requirements (non-contractual) are verbalized to the Contractor.

5. For projects in construction, who should be that starting point for initiating a modification? Should the CM contact the PM/DM?

   The decision to issue a post-award modification should be managed by the CM with support by the PM (budget)/DM (technical). The FEAD/ROICC office is responsible for execution of projects post-award. If the Contractor's modification proposals are unreasonable for the configuration and documentation for products already being provided, then it stands to reason to not award. In order to circumvent this situation, it would be prudent to discuss the details of UFGS 25 50 00.00 20 with the Contractor to ensure they understand the requirements prior to issuing the modification.

UFGS 25 50 00.00 20 COMPLIANCE QUESTIONS

6. Who answers questions, from Contractors about how to comply with cybersecurity submittal requirements as well as on the Cybersecurity Hygiene Checklist and Control Systems Inventory spreadsheet, CIO4?

   The Contractor should submit an RFI and as needed, CIO4 could assist with answering questions about the specification requirements of UFGS 25 50 00.00 20, especially about filling out the IP device inventory spreadsheet. The 'Data Dictionary' tab of the "NAVFAC Control System Inventory Spreadsheet" (available at http://www.wbdg.org/FFC/NAVGRAPH/graphtoc.pdf) provides a detailed description of the fields used in the inventory spreadsheet.

7. Although they are not "G" submittals, is anyone responsible for ensuring that cybersecurity submittals from Contractors are good enough, CIO4?

   The Contractor's Quality Control (CQC) representative is responsible for ensuring the cybersecurity submittals satisfy the requirements of UFGS 25 50 00.00 20. CIO4 will receive and retain the cybersecurity submittals for the eventual Interim Secure determination.

8. What does the Project Manager (PM), Design Manager (DM), and Construction Manager (CM) do if support from CIO4 is not provided for Questions 3, 4, and 6?

   If no support is provided from CIO for assistance with UFGS 25 50 00.00 20 editing, participation at the Pre-Construction Meeting, or assistance with addressing RFIs, the CM and PM/DM should document this in the project file and proceed with the project.

APPLICABILITY OF UFGS 25 50 00.00 20

9. ITG 2017-01 is pretty clear that this applies only to Navy-funded construction – are there any circumstances where we should consider applying for other projects funded from other services? Does this apply to Marine Corp construction?

   The requirement for the Cybersecurity Hygiene Checklist (i.e., Interim Secure) originates from the joint CNIC/NAVFAC letter, making this applicable only to projects that will result in CNIC facilities. In general, UFGS 25 50 00.00 20 is not applicable to MCICOM projects. However, if these projects will eventually be CNIC facilities, then a discussion needs to occur with the MCICOM Resource Sponsor to determine acceptability to invoke UFGS 25 50 00.00 20.

10. Where USACE is the MILCON D&C Agent (Japan), should ITG 2017-01 be forwarded to them so they follow it for Navy MCON in Japan?

    The requirement for UFGS 25 50 00.00 20 is applicable only to CNIC facilities, regardless of the Design and Construction Agent.

11. Confirm that ITG 2017-01 is not applicable for Air Force, DLA, DISA projects.

    The requirement for UFGS 25 50 00.00 20 is applicable only to CNIC facilities. In general, UFGS 25 50 00.00 20 is not applicable to Air Force, DLA, and DISA projects. However, if these projects will be located on a CNIC-maintained joint base, then a discussion needs to occur with the Defense Agency Resource Sponsor to determine acceptability to invoke UFGS 25 50 00.00 20.

12. Confirm that ITG 2017-01 is applicable to Seabee and USMC Defense Policy Review Initiative (DPRI) projects.

    The requirement for the Cybersecurity Hygiene Checklist (i.e., Interim Secure) originates from the joint CNIC/NAVFAC letter, making this applicable only to projects that will result in CNIC facilities. In general, UFGS 25 50 00.00 20 is not applicable to MCICOM projects. However, if these projects will eventually be CNIC facilities, then a discussion needs to occur with the MCICOM Resource Sponsor to determine acceptability to invoke UFGS 25 50 00.00 20.

UFGS 25 50 00.00 20 UTILIZATION QUESTIONS

13. Shall Specification Section 01 30 00 be modified to include Section "1.9.1 Cybersecurity of Control Systems..." under Section 1.9 PRECONSTRUCTION MEETING?

    Yes. This is just to highlight the requirement, not to go into in-depth discussion.

14. Shall Specifications of applicable equipment and systems be modified to include Section "1.X SUBMITTALS..." and "3.X CYBERSECURITY..."?

    Yes. This is to ensure that there is linkage to UFGS 25 50 00.00 20 and that the appropriate sub-contractors provide the cybersecurity submittal for their control system.

15. UFGS 25 50 00.00 20 Section 1.2.4.1.b states, "Provide the latest Operation System (OS) software for the control system. (Task ID #2)" This appears to be a Contractor action. The corresponding Cybersecurity Hygiene Checklist Task ID #2 states, "The operational community shall perform inventory checks using the provided baseline, reporting results in an actionable fashion." Is this the same action and who marks the Hygiene Checklist Task ID #2 as completed, the Contractor or the operational community (PW, User, CIO?)

    The Cybersecurity Hygiene Checklist Task ID #2 targets the Government User. UFGS 25 50 00.00 20 will be revised to remove the Task IDs that is not appropriate for a Contractor to complete. The Contractor, or the appropriate sub-Contractor, will mark the Cybersecurity Hygiene Checklist complete ('Completed? Y/N' and 'Responsible Party' columns) and CIO4 would indicate their concurrence in the Comment block, ideally during the Cybersecurity Field Verification (3.1.1).

16. Are Cybersecurity Hygiene Checklist Task IDs #4-17 targeting the Contractor's Users/Accounts, or those of the eventual Users/Operators? If the latter, who is the Responsible Party for the Checklist?

    The Cybersecurity Hygiene Checklist Task IDs #4-17 targets the Government User. UFGS 25 50 00.00 20 will be revised to remove the Task IDs that is not appropriate for a Contractor to complete.

17. Is CIO4 the POC for answering questions on the Cybersecurity Hygiene Checklist and Control Systems Inventory spreadsheet?

    The Contractor should submit an RFI and as needed, CIO4 could assist with answering questions about the specification requirements of UFGS 25 50 00.00 20, especially about filling out the IP device inventory spreadsheet. The 'Data Dictionary' tab of the "NAVFAC Control System Inventory Spreadsheet" (available at http://www.wbdg.org/FFC/NAVGRAPH/graphtoc.pdf) provides a detailed description of the fields used in the inventory spreadsheet.

18. Is the UFGS 25 50 00.00 20 correct in that we need to add SD-09 checklist submittal verbiage to every ICS-related spec section? Is it good enough to have all the checklists come in with the single report required in UFGS 25 50 00.00 20?

    The language regarding the SD-09 verbiage in related specification sections is meant to ensure that there is linkage to UFGS 25 50 00.00 20 and that the appropriate sub-contractors provide the cybersecurity submittal for their control system. While it seems duplicative, this will ensure that no control systems are overlooked. UFGS 25 50 00.00 20 consolidates the individual submittals from the control system specifications to form a comprehensive cybersecurity submittal.

19. For FY19 projects, will there be an ITG #2 issued for use?

    Once a full version of the cybersecurity UFGS (currently under development) is received, a determination will have to be made about the feasibility of using that as a basis for ITG #2. The goal is to provide criteria that complement UFC 4-010-06 as soon as reasonably possible.

20. The specification says "Provide office code, usually CIO4, contact phone number, and address of NAVFAC CIO in brackets". Our team does not have this information. The comment is in reference to providing an extra submittal to the CIO. If this information is not available, can we delete this requirement?" Shall Specification 01 30 00 be modified to include Section "1.9.1 Cybersecurity of Control Systems..." under Section 1.9 PRECONSTRUCTION MEETING? What's the intent for this extra submittal?

    The requirement cannot be deleted. This spec is to require the Contractor to make the facility "interim secure" for the Operational Technology building systems (as in OT vs IT). CIO4 currently has the responsibility to "interim secure" existing facilities based on a prioritized listing for all Navy facilities for their area of responsibility.

    This specification has two goals: (1) assist with reaching an Interim Secure level for new facilities and (2) provide that information to CIO4. So the CIO4 contact cannot be deleted. Being that this is another POC requirement for NAVFAC projects, the PM needs to coordinate the CIO4 point of contact, which is expected to be at the FEC level if not at the station, and that they will need that POC for each and every project in their AOR.

21. What is the recommended method of incorporating UFGS 25 50 00.00 20 into a Design-Build package?

    Include the following three sentences as the last paragraph in PART 3 - PROJECT PROGRAM, paragraph 2.3.7 Cybersecurity:

    > ***"Incorporate elements of the NAVFAC Cybersecurity Hygiene Checklist into contract specifications by using SECTION 25 50 00.00 20, CYBERSECURITY OF FACILITY-RELATED CONTROL SYSTEMS.***
    >
    > ***CIO4 Point of Contact to be utilized in SECTION 25 50 00.00 20 is:***
    >
    > ***[office code, usually CIO4,***
    >
    > ***contact phone number, and***
    >
    > ***address of NAVFAC CIO POC]***
    >
    > ***Submit Cybersecurity Plan and Cybersecurity Hygiene Report in accordance with SECTION 25 50 00.00 20."***