



C2 Security Certification Requirements

The commercial Business Objects™ (BO) application used to support M2, automatically ‘downloads’ data to the user’s PC in the process of building reports. Because this download may include sensitive data and the user does not control whether or not a download occurs, then the system to which the download is occurring must have at least the minimum security in place for protecting sensitive data. Under DoD and Service requirements, the local commander and appointed information system security officer are responsible for ensuring that automated systems under their control that store or process sensitive data meet minimum security standards. Normally, the process through which this is accomplished is a local certification/accreditation of the system at the C2 security level (as described in the DoD 5200.28-STD; known as the “Orange Book”). Under legal and regulatory guidance, the EI/DS PO, prior to allowing the transfer of sensitive data, must have assurance that the data will continue to be protected as prescribed by law and regulation. Thus, the requirement exists for a local commander or security officer to verify that any PC being used for sensitive data transfer is configured to meet minimum security requirements.

Some organizations do not have a process in place for obtaining local C2 level certification of a PC. In order to expedite the registration process, one of the following three statements, signed by your Organization Security Officer or Commanding Officer, will be accepted in order for you to obtain your account:

- a. “The PC/Workstation assigned to (User’s Full Name/Identity) has been certified to be C2 compliant in accordance with DoD, Service, and local requirements; a copy of the certification or a statement by local Commander or Security Officer attesting to the **certification is attached.**”

or

- b. “The PC/Workstation assigned to (User’s Full Name/Identity) has removable media (**identify type of media**, i.e., Jaz Drive, CD-RW) that will be used for EI/DS downloads; all such media will be protected in accordance with applicable requirements for handling and storage of sensitive data and marked accordingly (i.e., ‘FOUO’).”

or

- c. “The PC/Workstation assigned to (User’s Full Name/Identity), although not currently certified to be C2 level compliant, has been configured to meet as many of the DoD/Service mandated security requirements as feasible. Other mitigating actions (as listed below) are being taken to ensure that EI/DS data is protected when downloaded. **I have reviewed the mitigating actions and accept the risk to sensitive data associated with the implementation of those actions.**”

[NOTE: For statement ‘c’ above, mitigating actions could be restricting physical access to the PC by placement in an office that is locked when not occupied, removal of the PC from network automatic logins, ensuring the PC is removed from network activity when not in use, and/or other measures deemed appropriate by local authorities.]

The above statements are examples of what the Program Office believes to be appropriate and should not be considered as required statements. A similar type statement in the words of your organization's Commander or Security Officer may also be acceptable.