ACCESS TO SEIWG PRODUCTS

Operational Security

The following shall be followed as Operational Security (OPSEC) regarding individual requests to the SEIWG SharePoint website and futures SEIWG sites and information for public release:

International Traffic in Arms Regulations (ITAR)

The Department of State Office of Defense Trade Controls License (DDTC) governs the commercial export of US Munitions List items including hardware, technical data and defense services. There is no list of preapproved countries. If the information meets the criteria for technical data as defined in part 120.10 of the ITAR, a license is required. Unclassified tech data (including FOUO) needs a DSP-5 export license. Classified technical data (Confidential and above) need a DSP-85 export license.

After consulting with a DoS ITAR representative, the SEIWG has concluded that our Interoperability Standards documentation clearly falls into the technology category. "ITAR controlled technical data is defined in Part 120.10 of the ITAR." Below is what is outlined in Section 120.10 of the ITAR:

120.10 Technical Data

a) Technical data means, for the purposes of this subchapter:

i) Information, other than software as defined in 120.10(a)(4), which is required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of defense articles. This includes information in the form of blueprints, drawings, photographs, plans, instructions, or documentation.

ii) Classified information relating to defense articles and defense services;

iii) Information covered by invention secrecy order;

iv) Software as defined in 121.8(f) of this subchapter directly related to defense articles;

v) This definition does not include information concerning general scientific, mathematical or engineering principles commonly taught in schools, colleges and universities or information in the public domain as defined in 120.11. It also does not include basic marketing information on function or purpose or general system descriptions of defense articles.

DoD may have other arrangements or approval for the release of such data to foreign allies, for example under FMS cases. The SEIWG will place the burden of discovery and proof of any such arrangements on the requesting foreign entity. If proof is presented, the SEIWG will then

validate the information provided with DoD authorities and determine if any formal process must be pursued to document the transfer of information. After establishing that we are cleared to release the information, the SEIWG will share the requested information.

Based on this conclusion, the SEIWG will require that all foreign interests that request access to the SEIWG SharePoint website or the Interoperability Standards comply with this process.

Public Releases

Any documents that will be publically released will require formal approval. The SEIWG Operations Manager (OM) will provide initial review and recommendation for release and coordinate with the PSEAG support team to obtain the approval of the PSEAG Chair before ultimately being approved for public release. If a SEIWG artifact has been approved by the PSEAG for release, Services will follow the constraints of their PAO policies before distributing the material.

SEIWG SharePoint Website

The SEIWG SharePoint will be the centralized repository for the SEIWG. The SEIWG SharePoint website provides a common platform to ensure all documents and data are the most current version and released formats. Access to the SEIWG SharePoint website will be granted by the Operations Manager and Project Engineer.

SEIWG SharePoint Website Vetting Policy

- All DoD government , SEIWG Organic Team and Non-Organic Team representatives that possess a .mil email extension:
    - Entitled to access the SharePoint after they submit their application
- All DoD contractors or industry partners (e.g. vendors and manufacturers), who do not possess a .mil email extension, even if the SEIWG has a high level of confidence that they are performing work for the DoD or other federal government agency on one or more contracts:
    - The request will require that a DoD government sponsor and contact information be included
    - The SEIWG will confirm sponsorship and will specify to the government point-of-contact that it is his or her responsibility to submit an application for their individual access and it is his or her responsibility to manage and control distribution to his or her contractor or industry partner
- U.S. or Canadian Industry Partners that participate in the JCP and have entered into a Technical Data Agreement with the SEIWG will not be granted access to the SharePoint; however, in order to obtain SEIWG artifacts, SEIWG artifacts will be provide via AMRDEC.
- All Foreign Nationals or Foreign Owned Businesses
    - The International Traffic in Arms Regulations (ITAR) process must be followed before SEIWG controlled artifacts will be released
    - If the ITAR process is approved, then only individual documents will be conveyed
    - Under no circumstance will a Foreign National or Foreign Owned business be granted access to the SEIWG SharePoint site