Supplemental Information – Policy References

Export Control Training Scenario – 2013 Awareness Training
Converging on Converting

Laser Technology/ITAR:
Reference: Laser technology specifically designed for military applications is regulated by International Traffic in Arms Regulations (ITAR).

Requirement: *ISS100.4.3, Comply With Export/Import Controls* – All technical data/information is export-controlled unless the information has been reviewed and determined to be publicly available information or public domain.

Information Protection/Review & Approval (R&A)/Export-Controlled Information:
Reference: Foreign nationals could potentially access information uploaded to an external site. Do not use external sites outside the Sandia firewall for PDF conversion.

Requirement: Records Management Manual, Chapter 3: Review & Approval, Section 1.2, Programmatic or Organizational Review and Approval Process – Any information being released to the public must be reviewed for classification and sensitivity. This process incorporates reviews for intellectual property rights and partnerships and obtains the necessary approvals from derivative classifiers (DCs), Classification, managers overseeing Sandia's common look and feel standards, and designated line managers.

ISS100.1.1, Identify Classified Information – Documents or material approved for public release to an uncontrolled audience is designated as Unclassified Unlimited Release (UUR). An export compliance assessment is performed as part of the R&A process. From this assessment, there may be a determination made that the release of this information will require an export license.

Password-Protected Email:
Reference: Email transmittals containing Official Use Only (OUO) information require encryption to protect the data from unauthorized access. ECI information is a subset of OUO.

Requirement: *IM100.2.5, Identify and Protect Unclassified Information* – To transmit OUO information, such as ECI, over a network (including email), encrypt transmissions of OUO with Entrust or some other FIPS 140-2 compliant method (such as Office 2007–see UCI Information protection options for Office 2007) when sending outside of the sandia.gov domain.

IM100.2.5, Identify and Protect Unclassified Information, requires that **OUO information be encrypted if it is transmitted over a network.** As the encryption policy also pertains to unclassified mobile computing devices and media, the definition of mobile computing devices and media has also been clarified.

Email Marking:
Reference: Emails containing OUO information require marking to inform the recipient of control requirements. ECI information is a subset of OUO.

Requirement: *IM100.2.5, Identify and Protect Unclassified Information* – Mark documents per instructions under Control Official Use Only (OUO) Information. Freedom of Information Act (FOIA) Exemption 3 status for ECI applies. Add appropriate sentences under OUO label for further restrictive information. If a document is not properly marked, the potential for it to be improperly forwarded is high.