Mapping Between

Extended Package for Secure Shell (SSH), Version 1.0, 19-February-2016

and

NIST SP 800-53 Revision 4

Important Caveats

- **Product vs. System.** The Common Criteria is designed for the evaluation of products; the Risk Management Framework (NIST SP 800-37 Revision 1, DOD 8510.01) and associated control/control interpretations (NIST SP 800-53 Revision 4, CNSSI № 1253) are used for the assessment and authorization of mission systems. **Products cannot satisfy controls outside of the system context**. Products may support a system satisfying particular controls, but typically satisfaction also requires the implementation of operational procedures; further, given that systems are typically the product of integration of multiple products configured to meet mission requirements, an overall system assessment is required to determine if the control is satisfied in the overall system context.
- **SA-4(7).** Perhaps it is needless to say, but satisfaction of any NIAP PP supports system satisfaction of SA-4(7), which is the implementation of CNSSP № 11.
- **System context of supported controls.** For a conformant TOE to support these controls in the context of an information system, the selections and assignments completed in the TOE's Security Target must be congruent with those made for the supported controls. For example, the TOE's ability to generate audit records only supports IA-3 to the extent that the TSF is used to connect to a remote device that is included in the set of "organization-specific and/or types of devices" assigned by that control. The security control assessor must compare the TOE's functional claims to the behavior required for the system to determine the extent to which the applicable controls are supported.

Common Criteria Version 3.x SFR		**NIST SP 800-53 Revision 4 Control(s) Supports**		**Comments and Observations**
FCS_COP.1(1)	**Cryptographic Operation – Encryption/Decryption**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE has the ability to perform AES encryption and decryption based on FIPS and NSA-approved standards.
FCS_SSH_EXT.1	**SSH Protocol**	N/A	N/A	This SFR is a stub that is intended to prompt the ST author to choose whether the TOE implements the SSH protocol as a client, server, or both. The

				specific security functionality implemented by the TOE is dependent on which of these choices is made.
Optional Requirements				
N/A	**N/A**	**N/A**	**N/A**	**N/A**
Selection-based Requirements				
FCS_SSHC_EXT.1	**SSH Protocol-Client**	AC-17(2)	**Remote Access:** Protection of Confidentiality/Integrity Using Encryption	The SSH client protocol implemented by the TOE provides confidentiality and integrity for remote access.
		IA-2	**Identification and Authentication (Organizational Users)**	A conformant TOE may use its SSH client functionality to interact with a remote system on behalf of an organizational user.
		IA-3	**Device Identification and Authentication**	A conformant TOE may use its SSH client functionality to establish a static or as-needed connection to a specific remote device that is authenticated using a public key and/or X.509 certificate (instead of an administrator-supplied credential), which supports this control.
		SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE has the ability to ensure the confidentiality and integrity of information transmitted between the TOE and another trusted IT product.
		SC-8(1)	**Transmission Integrity:** Cryptographic or Alternate Physical Protection	The TOE's use of SSH supports a cryptographic method of protecting data in transit.
		SC-13	**Cryptographic Protection**	The TOE provides cryptographic methods to secure data in transit

				which may satisfy organization-defined uses if the functionality claimed by the TSF is consistent with organizational requirements.
FCS_SSHS_EXT.1	**SSH Protocol-Server**	AC-17(2)	**Remote Access:** Protection of Confidentiality/Integrity Using Encryption	The SSH client protocol implemented by the TOE provides confidentiality and integrity for remote access.
		IA-2	**Identification and Authentication (Organizational Users)**	A conformant TOE provides SSH server functionality that enforces identification and authentication of organizational users attempting to access the TSF.
		SC-8	**Transmission Integrity**	A conformant TOE has the ability to ensure the confidentiality and integrity of information transmitted between the TOE and another trusted IT product.
		SC-8(1)	**Transmission Integrity:** Cryptographic or Alternate Physical Protection	The TOE's use of SSH enforces a cryptographic method of protecting data in transit.
		SC-13	**Cryptographic Protection**	The TOE provides cryptographic methods to secure data in transit which may satisfy organization-defined uses if the functionality claimed by the TSF is consistent with organizational requirements.
Objective Requirements				
N/A	**N/A**	**N/A**	**N/A**	**N/A**