

# TANTALUS SECURITY FRAMEWORK

## Audience & Purpose

This document is intended for utility organizations, auditing bodies and other organizations that require information on the cyber security of systems and networks developed and deployed by Tantalus. The focus of this document is to provide information on the current applicable standards that relate to the security of the smart grid and the applicability to the Tantalus product line.

Tantalus is committed to ensuring the security and resilience of its systems. As we strive to deliver value to utilities through fine-grained data, low-latency control and intelligent analytics, it is increasingly important to protect devices, interfaces, and systems from unwanted access, maintain the confidentiality of private data, guarantee the authenticity of devices and users, and ensure that key services and important functions remain available and operational. Accordingly, Tantalus regularly monitors and enhances its cybersecurity protocols and policies at both the technical and organizational levels so that we are taking the necessary and reasonable actions to be at or exceed industry standards in this regard.

## Standards

The “Tantalus Security Framework”, as described here, is guided by the normative standards listed at the end of this document. The overall framework for smart grid security is primarily guided by the recommendations in NIST IR 7628, “Guidelines for Smart Grid Cybersecurity”. The remaining documents in the normative standards list are a combination of standards and recommendations that provide specific areas of compliance or more detail on specific requirements.

In support of the Tantalus Security Framework, Tantalus performs periodic cybersecurity audits to ensure compliance with and adherence to the normative cybersecurity standards. These efforts apply not only the product capabilities and features, but also include reviews of internal processes and practices related to maintaining a current and effective cybersecurity approach to Tantalus’ product line.

Following NIST IR 7628, the Tantalus Security Framework aims to provide:

- Confidentiality – private data cannot be intercepted or accessed by an unauthorized party;
- Integrity – neither data nor software can be modified, either through malicious activity or corruption;
- Availability – maintaining operation of the system (head-end, network, endpoints and devices) in the event of attack or other potential interruption (e.g., environmental event or technological malfunction); and
- Authenticity – the identity of communicating devices and users is validated before allowing connection or access.

The following practices and technologies are core to the Tantalus Security Framework:

- Security In Depth & Zero Trust Models;
- Periodic cybersecurity audits with a third-party auditor with specialized experience in the smart grid sector;
- Certified hardware based cryptographic technology to ensure compliance with standards and to enable the highest performance of these functions on endpoint devices with limited resources;
- Virtualization to support disaster recovery and system management;
- Ongoing monitoring of publicly reported vulnerabilities through the CVE system (Common Vulnerabilities and Exploits);
- Internal processes and controls that ensure compliance with security protocols;
- Use of audited third-party systems such as Oracle Cloud Infrastructure; and
- Use of current operating systems and operating systems supported under the Linux Civil Infrastructure Project that have long term support for industrial applications.

## Normative Standards

The following is the list of standards utilized in connection with audits of Tantalus' systems:

Standard	Date of Issue	Description
NIST IR 7628 Rev. 1	Sep 2014	Guidelines for Smart Grid Cybersecurity Vol 1 - Smart Grid Cybersecurity Strategy, Architecture, and High-Level Requirements Vol 2 - Privacy and the Smart Grid Vol 3 - Supportive Analyses and References Announcement and Draft Publication
FIPS 140-3	Mar 2019	Security Requirements for Cryptographic Modules
FIPS 180-4	Mar 2012	Secure Hash Standard (SHS)
FIPS 186-4	Jul 2013	Digital Signature Standard (DSS)
FIPS 196	Feb 1997	Entity Authentication Using Public Key Cryptography
FIPS 197	Nov 2001	Advanced Encryption Standard (AES)
NEMA SG-AMI 1	R2020	Requirements for Smart Meter Upgradeability
NIST CSF Ver. 1.1	Apr 2018	Cyber Security Framework
SP-800-122	Apr 2010	Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)
SP-800-123	Jul 2008	Guide to General Server Security
SP-800-133	Dec 2012	Recommendation for Cryptographic Key Generation
SP-800-38C	Jul 2007	Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality
SP-800-38D	Nov 2007	Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC
SP-800-40 Rev. 4	Apr 2022	Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology
SP-800-41 Rev. 1	Sep 2009	Guidelines on Firewalls and Firewall Policy
SP-800-52 Rev. 2	Aug 2019	Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations
SP-800-53 Rev. 4	Jan 2015	Security and Privacy Controls for Federal Information Systems and Organizations
SP-800-56B	Aug 2009	Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography
SP-800-57	Jan 2016	Recommendation for Key Management
SP-800-60 Vol. 1 Rev. 1	Aug 2008	Guide for Mapping Types of Information and Information Systems to Security Categories
SP-800-60 Vol. 2 Rev. 1	Aug 2008	Guide for Mapping Types of Information and Information Systems to Security Categories: Appendices
SP-800-63-2	Aug 2013	Electronic Authentication Guideline
SP-800-77 Rev. 1	Jun 2020	Guide to IPsec VPNs
SP-800-82 Rev. 1	May 2013	Guide to Industrial Control Systems (ICS) Security
SP-800-82 Rev. 2	May 2014	DRAFT Guide to SCADA & Industrial Control Systems (ICS) Security Announcement and Draft Publication
SP-800-90 (A, B, C)	Sep 2019	Recommendation for Random Number Generation
SP-800-95	Aug 2007	Guide to Secure Web Services