

DATA IS POTENTIAL

# Seagate Supply Chain Standards and Operational Systems

Government Solutions | Henry Newman | May 9 2018



# Supply Chain Standards and Results

## Agenda

---

1. SUPPLY CHAIN REQUIREMENTS AND STANDARDS

2. SEAGATE APPROACH



# Supply Chain Requirements and Standards

DoD, NIST, FBI, ISO, O-TTPS



# Requirements for Information Relating to Supply Chain Risk

DoD Directive States

---

**What is supply chain risk?**

---

**DoD has clear definitions of risk**

---

**We see both direct and indirect risk every day that could impact the performance of national systems**



# FBI on Supply Chain

## Recommendations

**Federal agencies should develop a Supply Chain Risk Management (SCRM) strategy. It should include:**



**Known and  
emerging threats**



**Vulnerabilities**



**Organizational  
impacts**

The teams must be multi-disciplined and address SCRM, security, procurement, contract and administrative law, audit and finance, and facilities management



# Supply Chain Risk Management Practices for Federal Information Systems and Organizations

NIST Has a Whole Document on Supply Chain

**NIST has standards for ICT (Information and communications technology) that encompass all of Federal Government and contractors and is what DoD standards are based on NIST view 3 areas as critical**



Integrity



Resilience



Quality



# ISO Standards 28000:2007

## Review of What is in the ISO Standards for Supply Chain

**1.**

Establish, implement, maintain and improve a security management system

**2.**

Assure conformance with stated security management policy

**3.**

Demonstrate such conformance to others

**4.**

Seek certification/ registration of its security management system by an Accredited third party Certification Body; or make a self-determination and self-declaration of conformance with ISO 28000:2007

---

Companies doing business in the USA or Europe are going to be required being moving to follow supply chain standards



## ISO/IEC 20243-1:2018 Information Technology Mitigating Maliciously Tainted and Counterfeit Products

ISO Standard

**ISO also has a standard for mitigating maliciously tainted and counterfeit products.**

**Similar standards and regulation to NIST**

**Using counterfeit products has significant security risks**

**For computer products counterfeit has multiple meanings**

- Complete reengineered products
- Products that might have been previously used in other systems and recycled





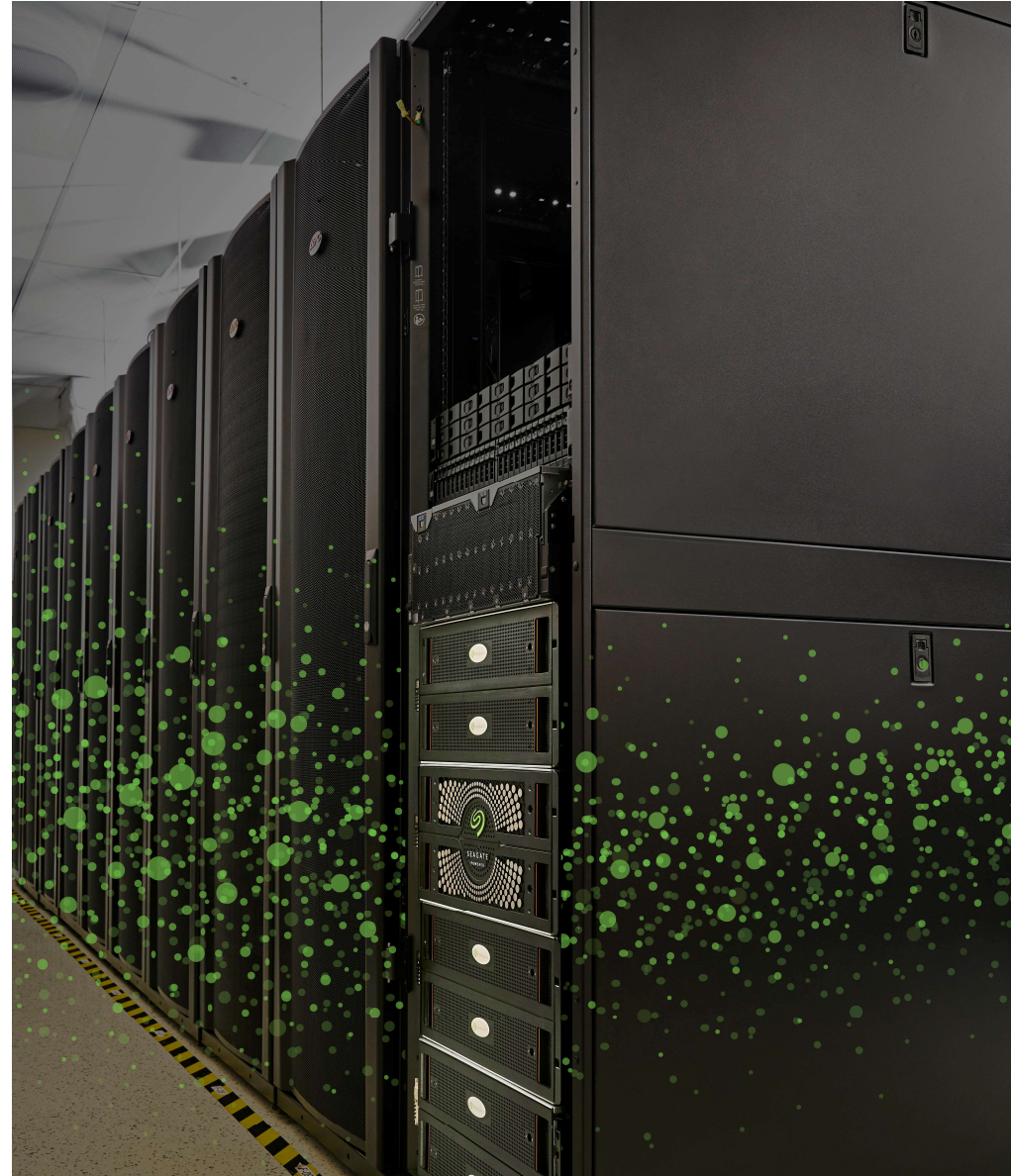
## What is the Aim of the O-TTPS

Open Trusted Technology Provider™ Standard

**OpenGroup has a clear definition called O-TTPS (Open Trusted Technology Provider Standard) for OEM and sub contractors**

- Very high cost in complex systems given audit required of sub-contractors
- Demonstration of conformance through this independent, voluntary O-TTPS Certification Program process provides formal recognition of an organization's conformance to this industry standard.

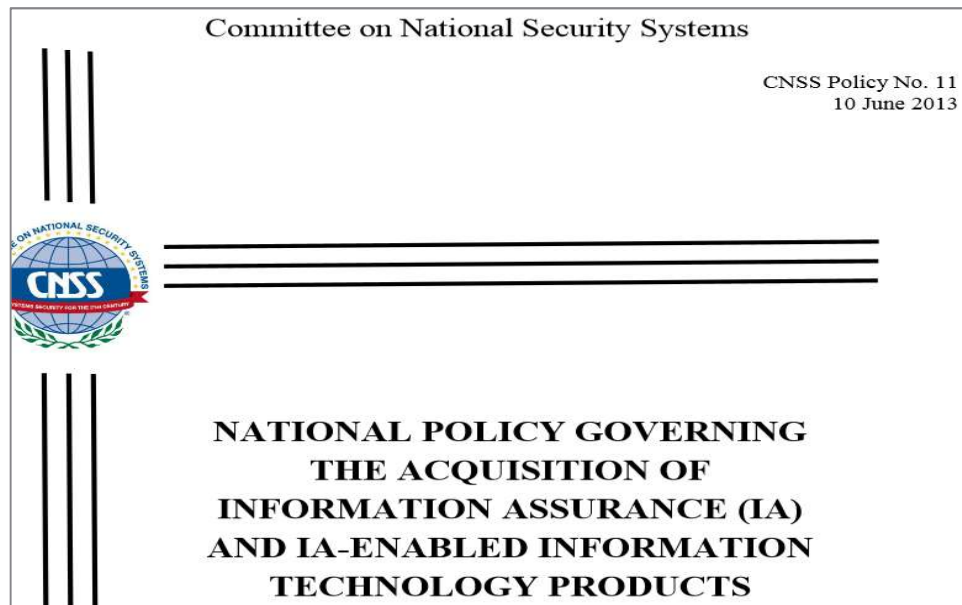
<https://ottps-cert.opengroup.org/>



## What Problem in the Market Does it Solve?

In the US, CC certification is mandated as a procurement prerequisite for defense and intelligence community use as per Committee on National Security Systems (CNSS) Policy #11.

**CNSS(Committee on National Security Systems) Policy#11 requires CC certification for all IA (Information Assurance) and IA-enabled devices.**



### FOREWORD

1. The attached policy supersedes National Security Telecommunications and Information System Security Policy (NSTISSP) No. 11, "National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products," dated January 2000 and revised in June 2003. CNSSP No. 11 clarifies the required evaluation processes applicable to Commercial-Off-The-Shelf (COTS) and Government-Off-The-Shelf (GOTS) IA and IA-enabled IT products that are used on U.S. National Security Systems (NSS) to protect the information therein.

a. The National Security Agency (NSA) and the National Institute for Standards and Technology (NIST) established the National Information Assurance Partnership (NIAP) program to implement and administer a process governing the testing and evaluation of COTS IA and IA-enabled IT products. The Director, NSA is responsible for implementing the NIAP as it applies to NSS to include approving processes for the evaluation of COTS products when they are to be used to protect information on NSS.

b. The Director, NSA, as the National Manager for NSS, is also directly responsible for establishing standards and criteria that GOTS IA and IT products must meet before they are used to protect NSS and the information therein.

2. Additional copies of this policy may be obtained by contacting the Secretariat or at the CNSS website: [www.cnss.gov](http://www.cnss.gov).



# Seagate Approach to Supply Chain

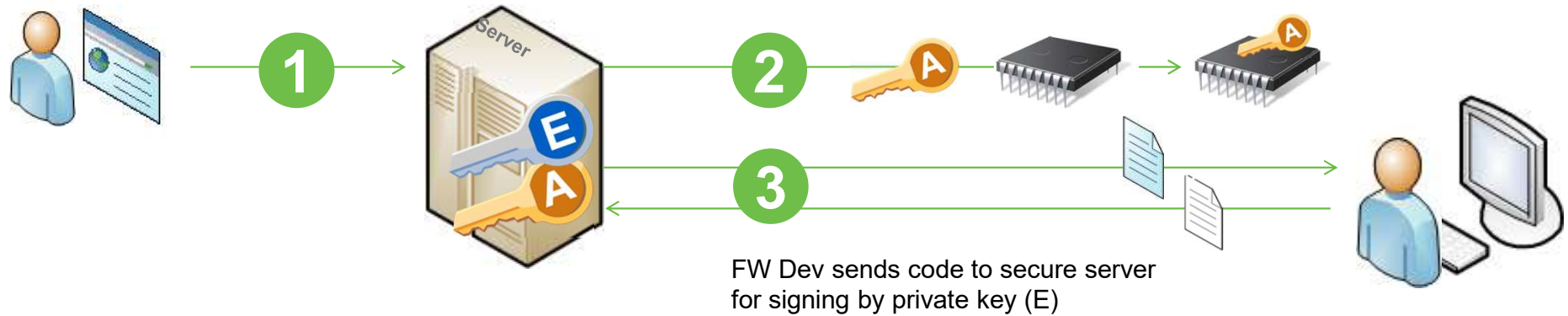
Firmware, Common Criteria, FIPS

## Secure Boot Process 2

Security Officer generates key pair in secure server in security module

Secure server secures private key (E)

Public key (A) is embedded in ROM code during ASIC development

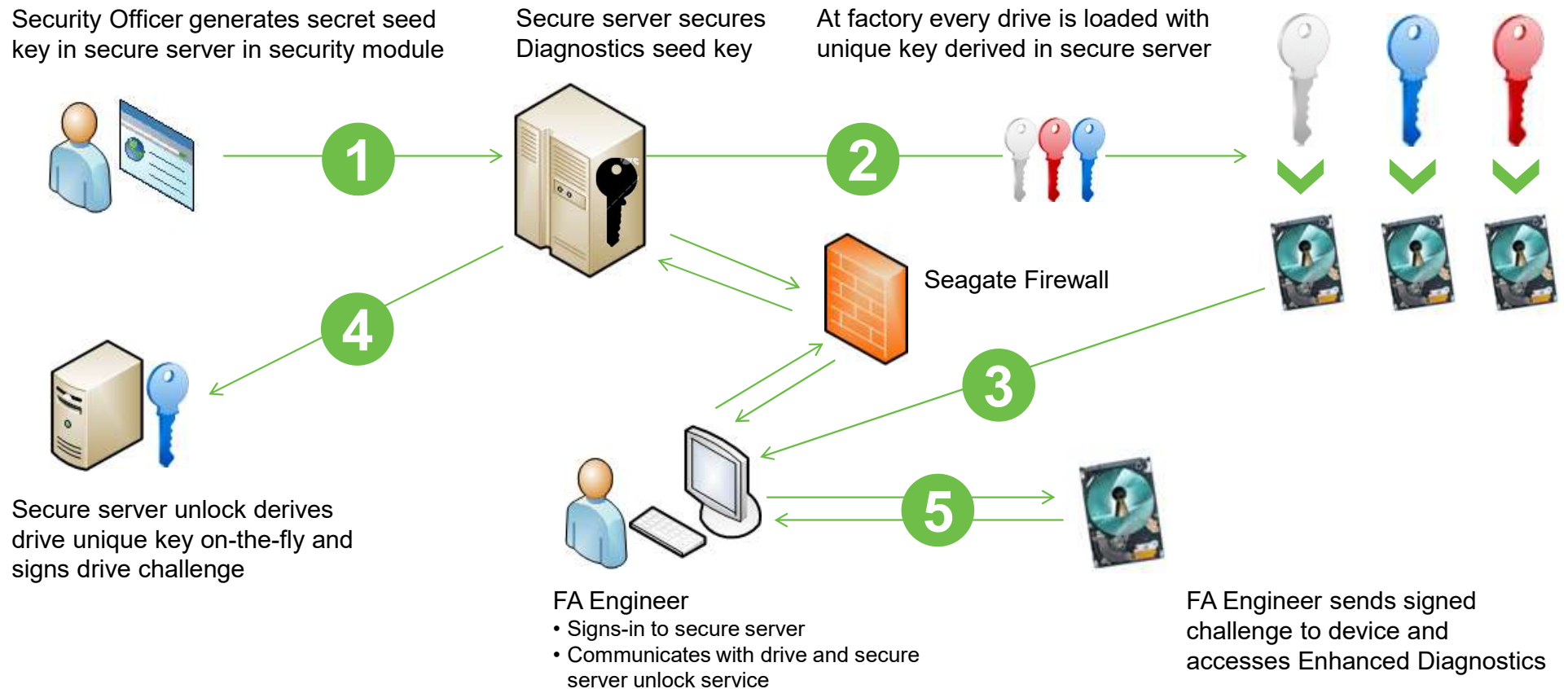


Signed firmware and SBP capable ASIC integrated in factory

At power-on, ASIC verifies firmware signature using embedded key (A)



# Diagnostics Command & Cross Segment FW Download Access



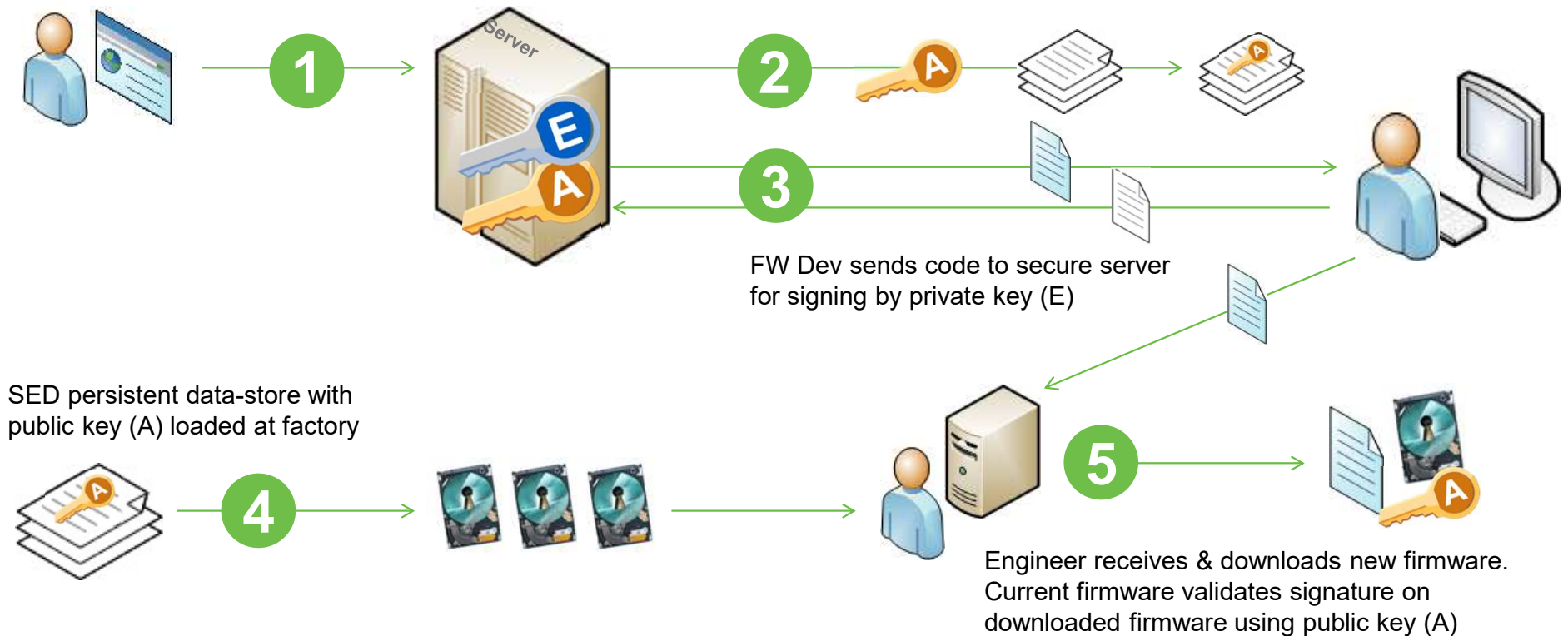


# Authenticated Firmware Download

Security Officer generates key pair in secure server in security module

Secure server secures private key (E)

Public key (A) is embedded in FIPS persistent data-store during development



# Supply Chain and 3rd Parties

The Need for Product, Component, and Services Security

Heightened Awareness & Sensitivity to Cybersecurity and Tainted Products

Customer Requirements

Brand Impact


Counterfeit Products

Standards & Certification Requirements

Origin, Authenticity, Chain of Custody

⇒ Attestable Product Security is now a stewardship requirement

[salesforce.com](https://www.salesforce.com) CEO Marc Benioff says, "We're in the early stages of a data science revolution, and executives of every type of business need to address the disruption and get serious about cybersecurity. **This clearly applies to our digital products....**" There is no finish line when it comes to cybersecurity."



Open Trusted Technology Provider™ Standard (O-TTPS) & Accreditation

FORTUNE INSIDERS: LENOVO

## Lenovo's Superfish fallout: Can we forgive and forget?

COMMENTARY by Brayden King MARCH 5, 2015, 7:30 AM EDT

Lenovo Group Ltd. has come under criticism for preinstalling its consumer laptops with the ad-serving Superfish software, which inserts ads into a variety of Web pages. The litigation stems from last year's revelations about security flaws in Superfish -- a program that inserts ads into a variety of Web pages.

## Has Equation Group hacked your hard drives? You won't be able to tell.

Infection can survive formatting and reinstalling the operating system

By Tim Greene Follow Network World Feb 28, 2015 10:21 AM PT

## Seagate Hard Disks Carry Malware

Posted on: November 13, 2007 at 11:36 am Posted in: Malware Author: Irene Vicente (Technical Communications)

In Taiwan, new Seagate Maxtor Basics hard drives carry malware, reports Taipei Times. The infected drives have a 500GB capacity and were reportedly manufactured in Thailand.

THE DAILY ONLINE EXAMINER

## Superfish Settles Privacy Lawsuit Over Adware-Infected Lenovos

by Wendy Davis @wendydavis, February 12, 2016, 1:59 PM

Adware company Superfish has agreed to pay \$1 million to settle a class-action privacy lawsuit on behalf of consumers who purchased Lenovo notebooks in late 2014 and early 2015, according to court papers filed on Thursday.

53 SHARES





# Common Criteria Certified Product Portfolio

## Overview

### What:

Common Criteria (CC) is an internationally recognized standard (ISO/IEC 15408) for assessing security functionality of information assurance (IA) and IA-enabled products.

### How:

A CC certification assures buyers that the process of specification, implementation and evaluation of any certified security product was conducted and proven in a thorough and standard manner.

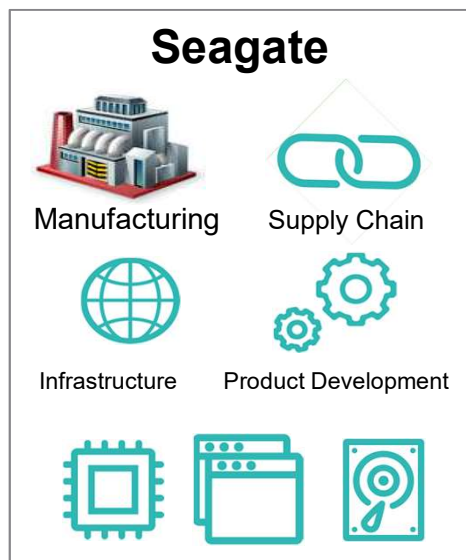
### Why:

CC certification is required for access to US and EU government markets. It can also be used as a competitive differentiator when marketing to non-government markets like finance, critical infrastructure and health care.





# Expanding Threats Landscape and Seagate's Continued Value Add



**Rogue Implants in Factory, Rogue Seagate Insider, Supply Chain Attack**

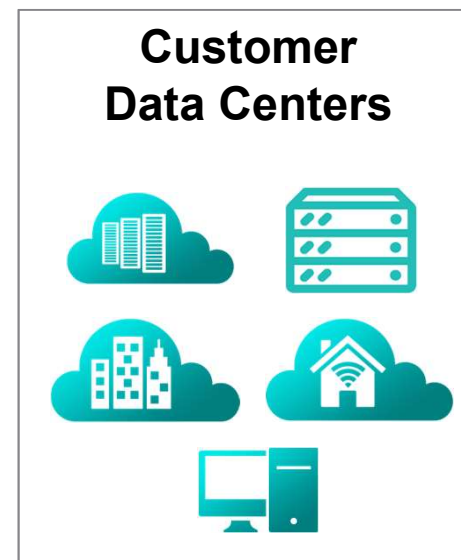
✓ **Rogue Firmware Detection Service**



**Warehouse Attack**

- Counterfeiting, Tampering of FW
- Unauthorized FW Update, Undetected Access

✓ **Attestation Service (in development)**



**Smash and Grab**

- Unauthorized Access to or Altering of User Data
- Key Material Compromise/Leakage

**End of Life / Decommissioning**

- Data exfiltration

✓ **ISE, SED & FIPS configs. with Seagate Cloud Key Mgmt. Solution**



Thank You

