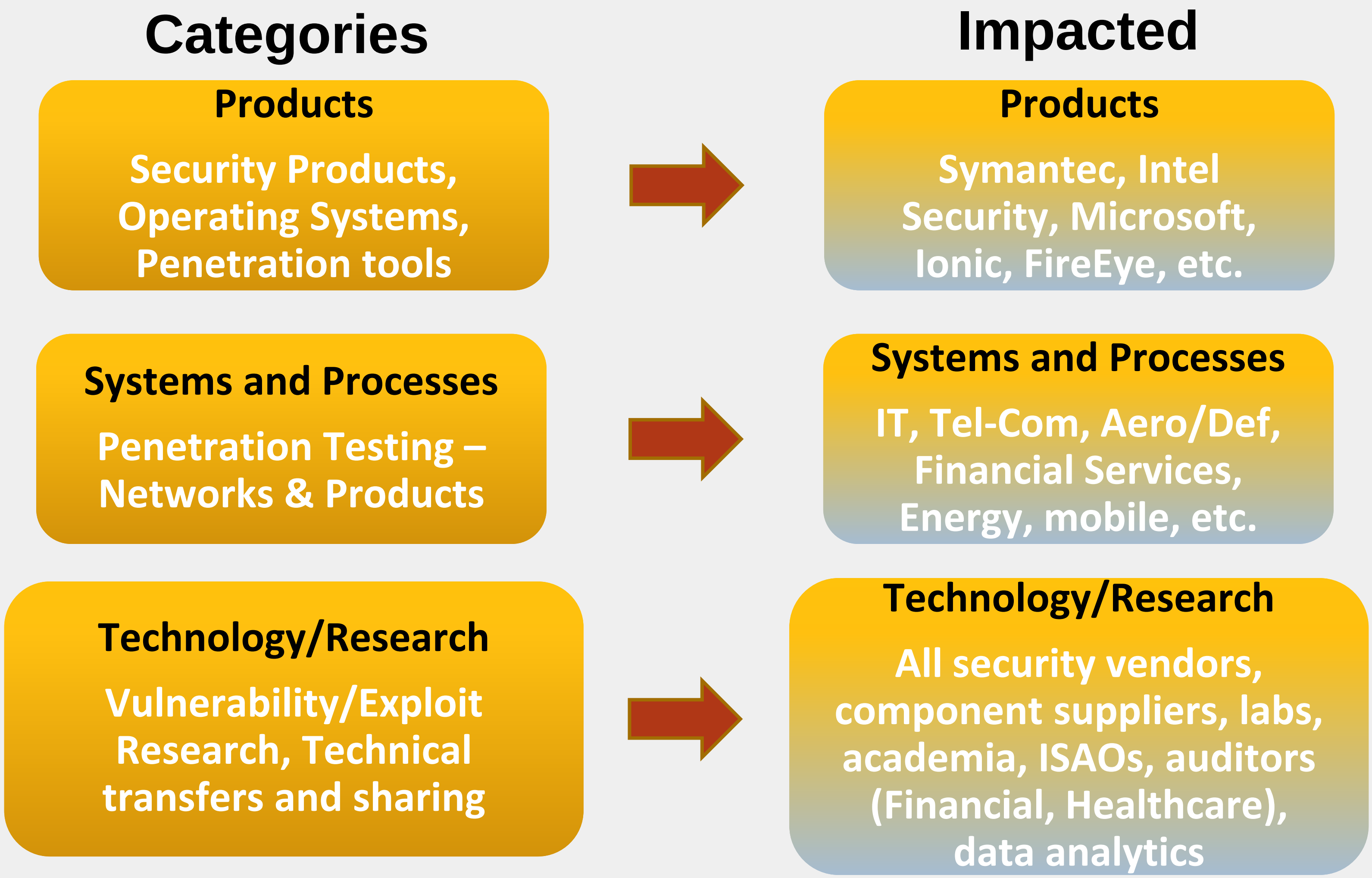
Three Broad Categories Of Control Impact



Categories

Products

Security Products, Operating Systems, Penetration tools

Systems and Processes

Penetration Testing – Networks & Products

Technology/Research

Vulnerability/Exploit Research, Technical transfers and sharing

Impacted

Products

Symantec, Intel Security, Microsoft, Ionic, FireEye, etc.

Systems and Processes

IT, Tel-Com, Aero/Def, Financial Services, Energy, mobile, etc.

Technology/Research

All security vendors, component suppliers, labs, academia, ISAOs, auditors (Financial, Healthcare), data analytics

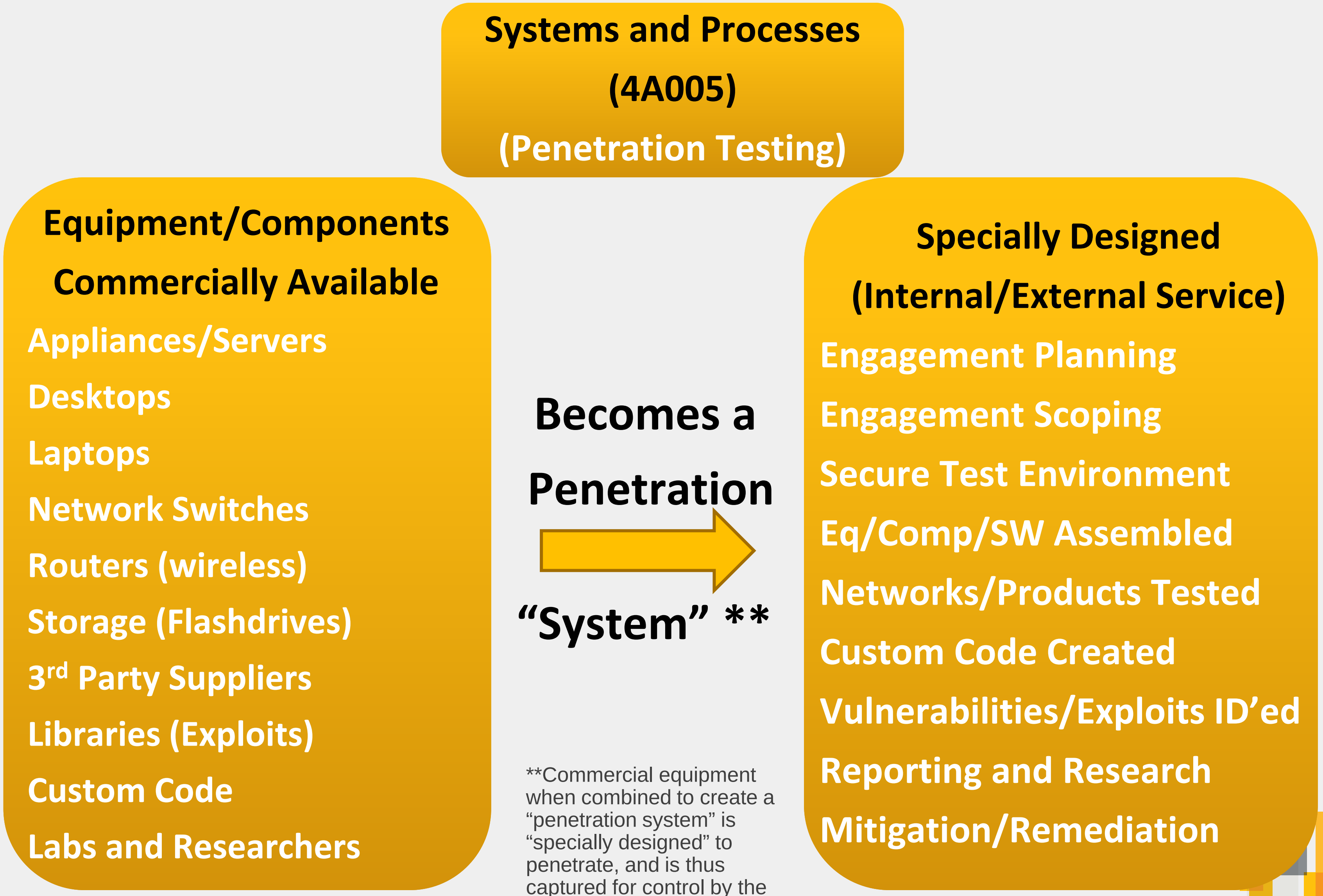
Intrusion Software Controls
(4A – Systems, Equipment, Components)

Proposed ECCN 4A005

- ‘‘Systems,’’ ‘‘equipment,’’ or ‘‘components’’ therefore, ‘‘specially designed’’ or modified for the generation, operation or delivery of, or communication with, ‘‘intrusion software’’

- Intrusion software: (Cat 4) “Software” “specially designed” or modified to avoid detection by ‘monitoring tools’, or to defeat ‘protective countermeasures’, of a computer or network-capable device, and performing any of the following:
  a) The extraction of data or information, from a computer or network-capable device, or the modification of system or user data; or
  b) The modification of the standard execution path of a program or process in order to allow the executions of externally provided instructions

Intrusion Software Impacts
(4A – Systems, Equipment, Components)



Systems and Processes

(4A005)

(Penetration Testing)

Equipment/Components

Commercially Available

Appliances/Servers

Desktops

Laptops

Network Switches

Routers (wireless)

Storage (Flashdrives)

3rd Party Suppliers

Libraries (Exploits)

Custom Code

Labs and Researchers

Becomes a

Penetration

“System” **

Specially Designed

(Internal/External Service)

Engagement Planning

Engagement Scoping

Secure Test Environment

Eq/Comp/SW Assembled

Networks/Products Tested

Custom Code Created

Vulnerabilities/Exploits ID’ed

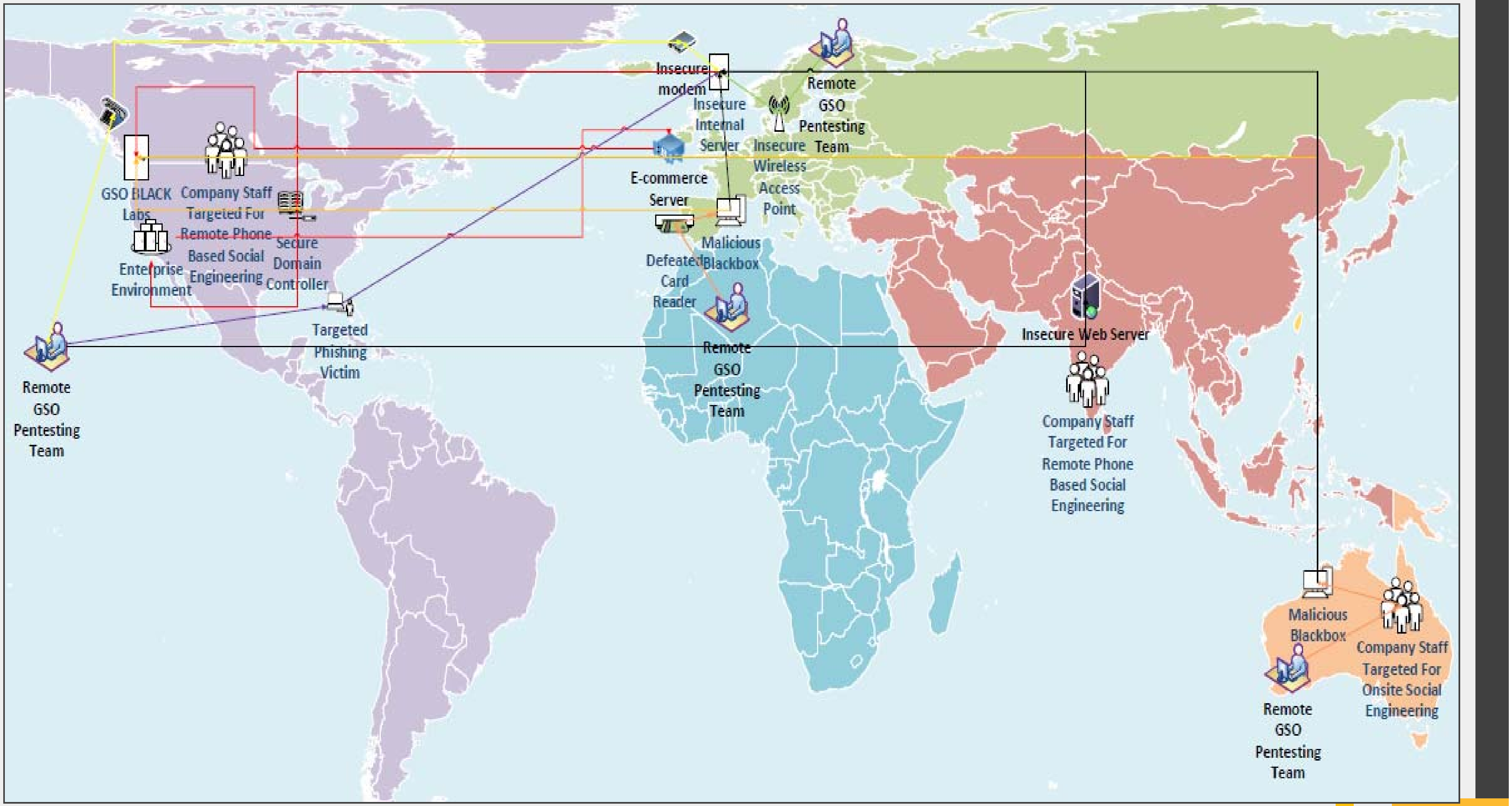
Reporting and Research

Mitigation/Remediation

**Commercial equipment when combined to create a “penetration system” is “specially designed” to penetrate, and is thus captured for control by the rule

Multi-National Network Penetration Testing

A Diagram of Geographical & Technological Complexity


Insecure modem
Remote GSO Pentesting Team
Insecure Internal Server
Insecure Wireless Access Point
E-commerce Server
GSO BLACK Labs
Company Staff Targeted For Remote Phone Based Social Engineering
Secure Domain Controller
Enterprise Environment
Malicious Blackbox
Defeated Card Reader
Remote GSO Pentesting Team
Targeted Phishing Victim
Remote GSO Pentesting Team
Insecure Web Server
Company Staff Targeted For Remote Phone Based Social Engineering
Malicious Blackbox
Company Staff Targeted For Onsite Social Engineering
Remote GSO Pentesting Team

Colored Lines indicate various methods of network attack such as phishing, poorly configured passwords on modems insecure card readers, insecure wireless modems, onsite social engineering (tailgating), etc.