black hat USA 2020

AUGUST 5-6, 2020

BRIEFINGS

Carrying our Insecurities with Us: the Risks of Implanted Medical Devices in Secure Spaces

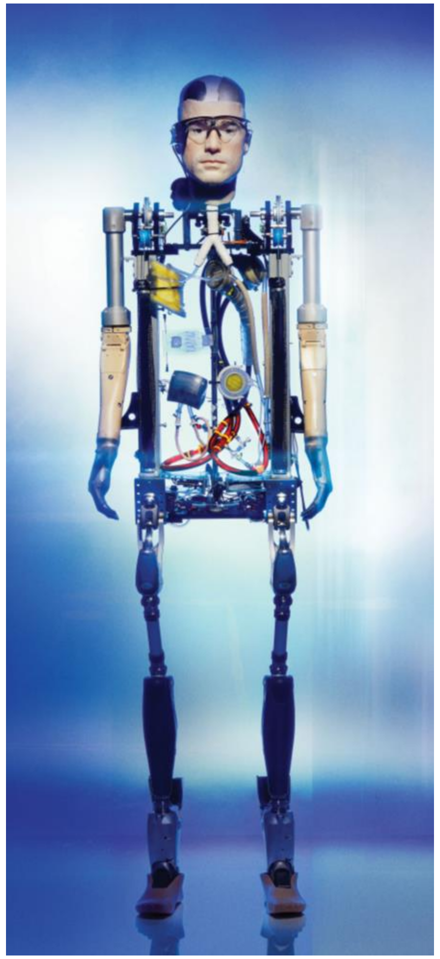
Alan J. Michaels, PhD

Research Professor and Director, Electronic System Lab

Virginia Tech Hume Center for National Security and Technology

The Risks of Implanted Medical Devices in Secure Spaces

Secure Compartmented Information Facility (SCIF)

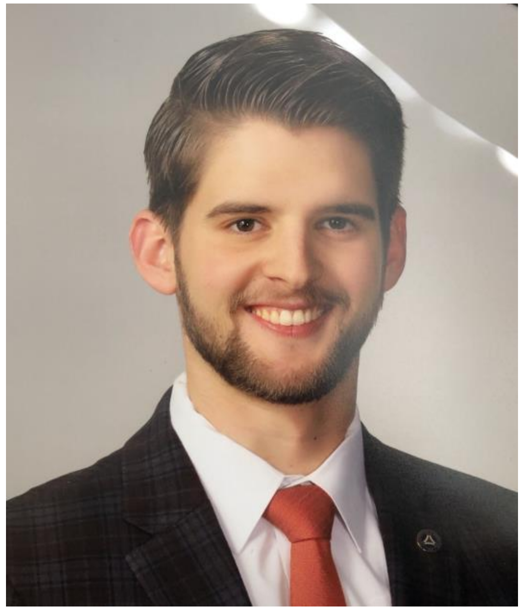


Implanted Medical Devices (IMDs)

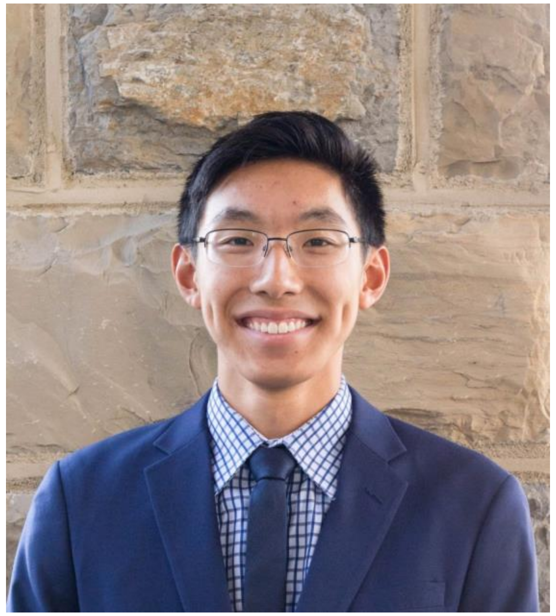
“SCIF of the Future” Research Team

Zoe Chen

Paul O’Donnell



Eric Ottman



Steven Trieu

Alan Michaels

ajm@vt.edu

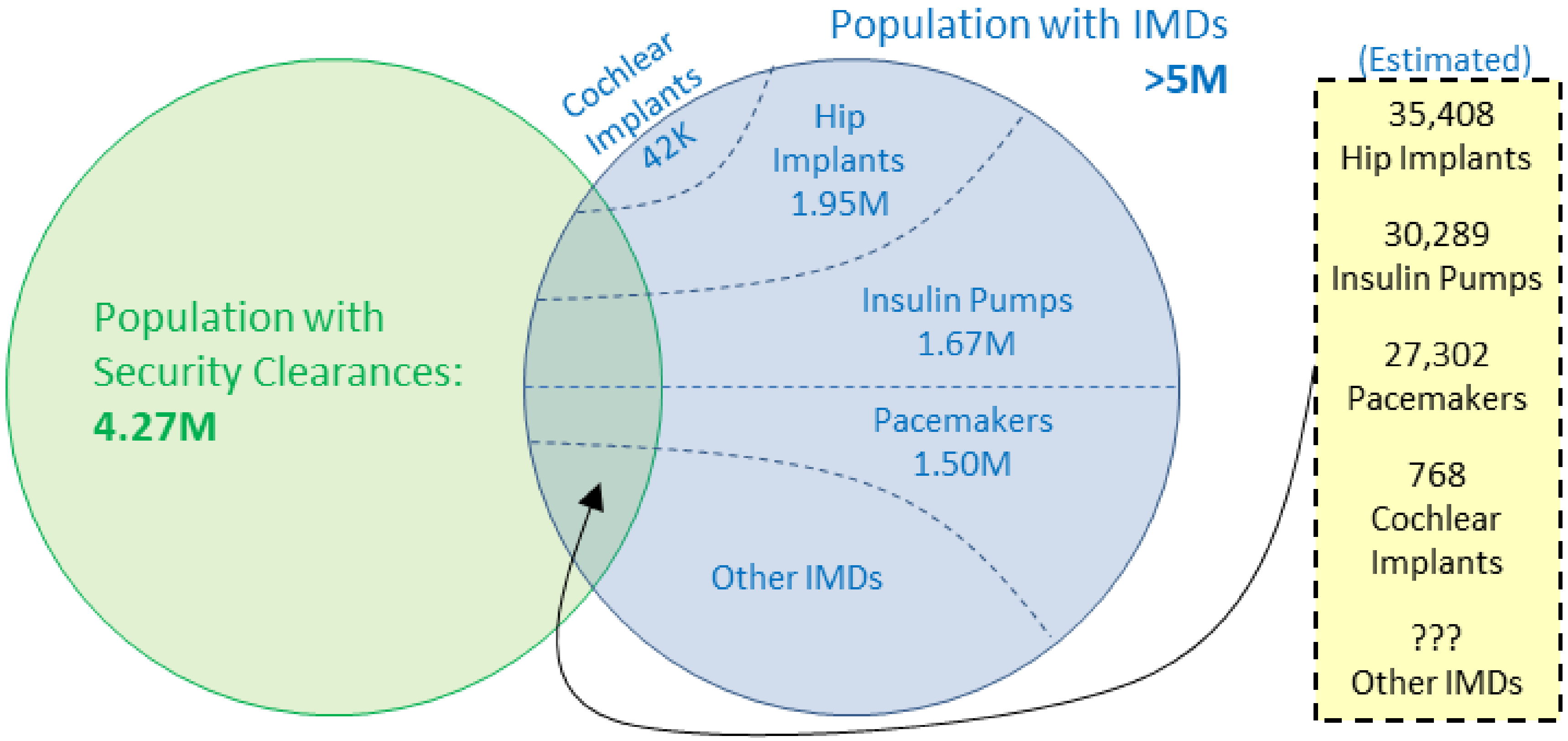
* Z. Chen, P. O’Donnell, E. Ottman, S. Trieu, and A. Michaels, *An Invisible Insider Threat: The Risks of Implanted Medical Devices in Secure Spaces*, National Intelligence University (NIU) Research Short, *in press*
* -, *Carrying our Insecurities with Us: The Risks of Implanted Medical Devices in Secure Spaces*, Black Hat whitepaper (available with this presentation)

Motivation

Security Clearance:

- Highly selective process
- 12-24 months and ~$75K
- Leads to unique expertise

Median age of National security workforce is >10 years older than average workforce



Rapidly increasing capabilities of connected implanted medical devices improving quality of life for millions

Unique class of industrial IoT

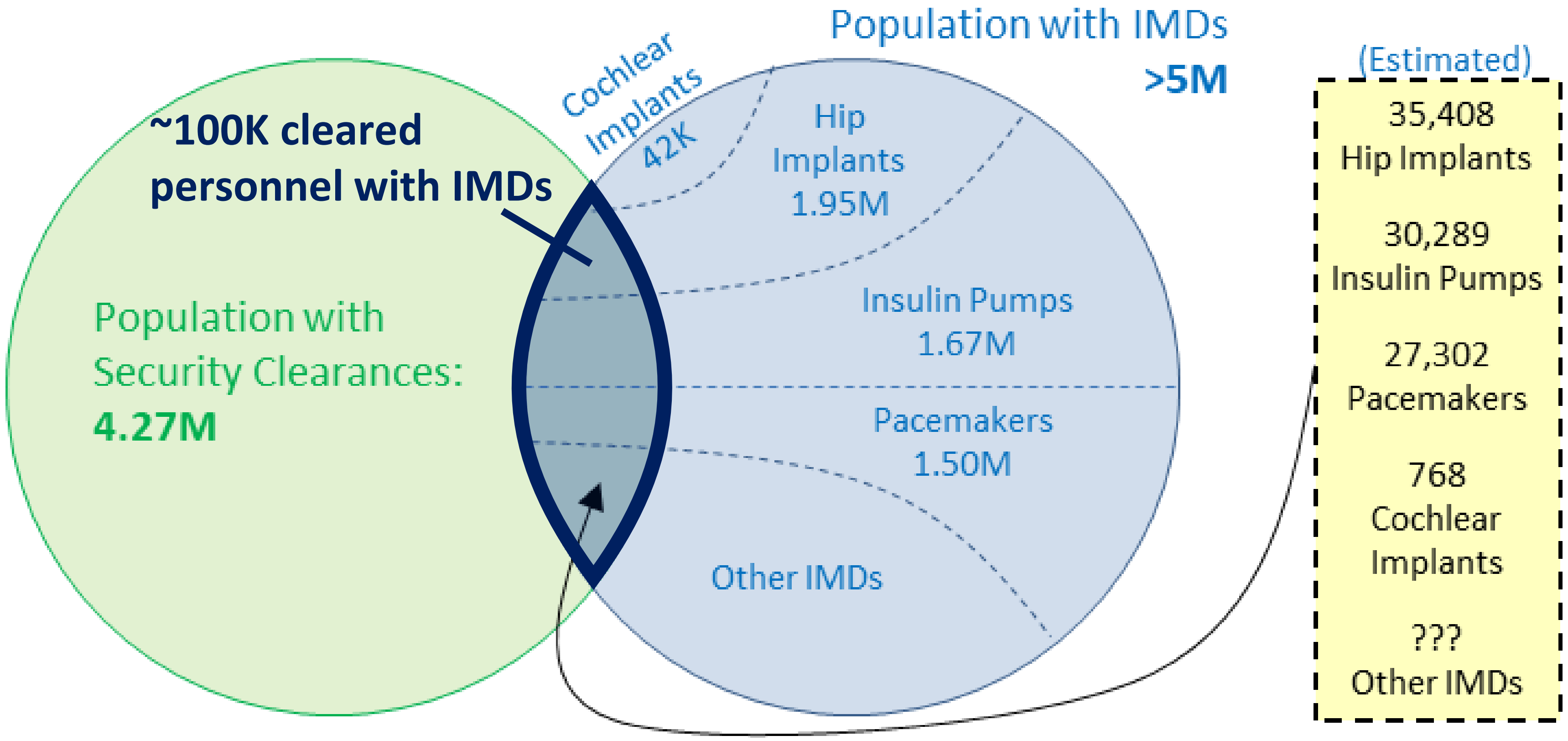
- Remotely configurable
- Bluetooth communications
- GPS tracking

Relatively few devices are designed / manufactured inside the United States

Motivation

Security Clearance:
- Highly selective process
- 12-24 months and ~$75K
- Leads to unique expertise

Median age of National security workforce is >10 years older than average workforce

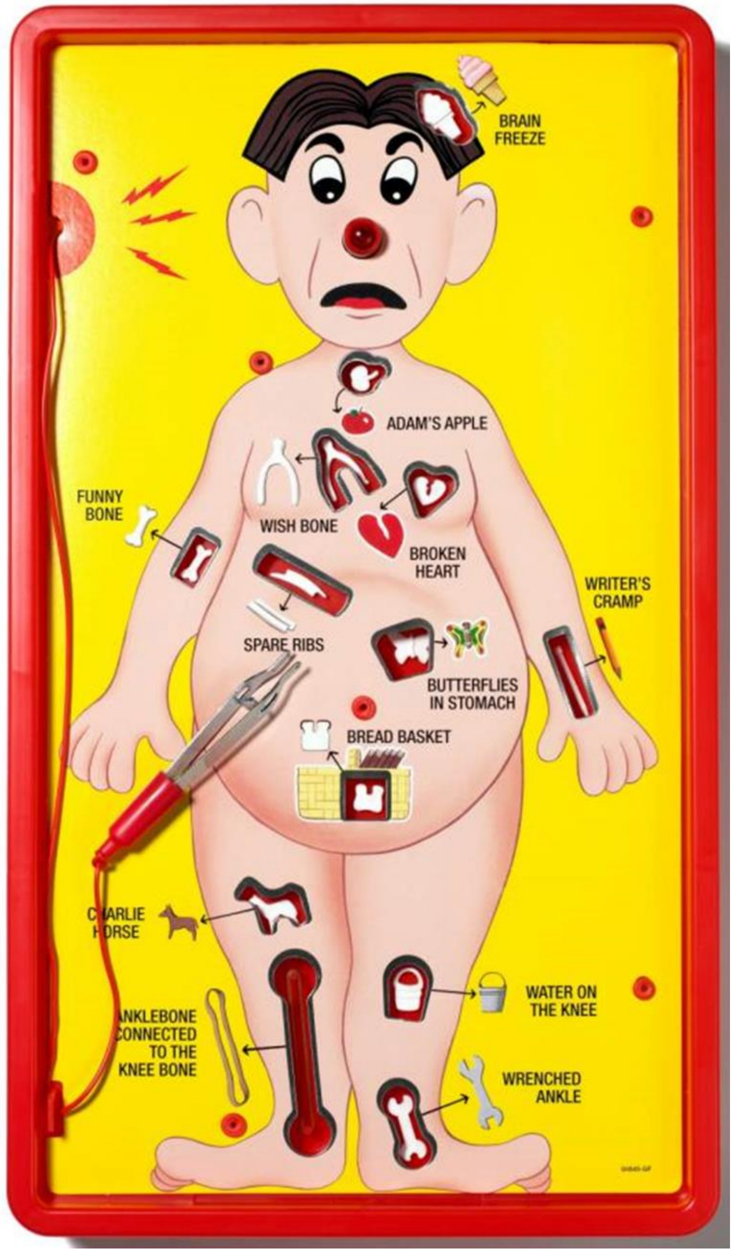


Rapidly increasing capabilities of connected implanted medical devices improving quality of life for millions

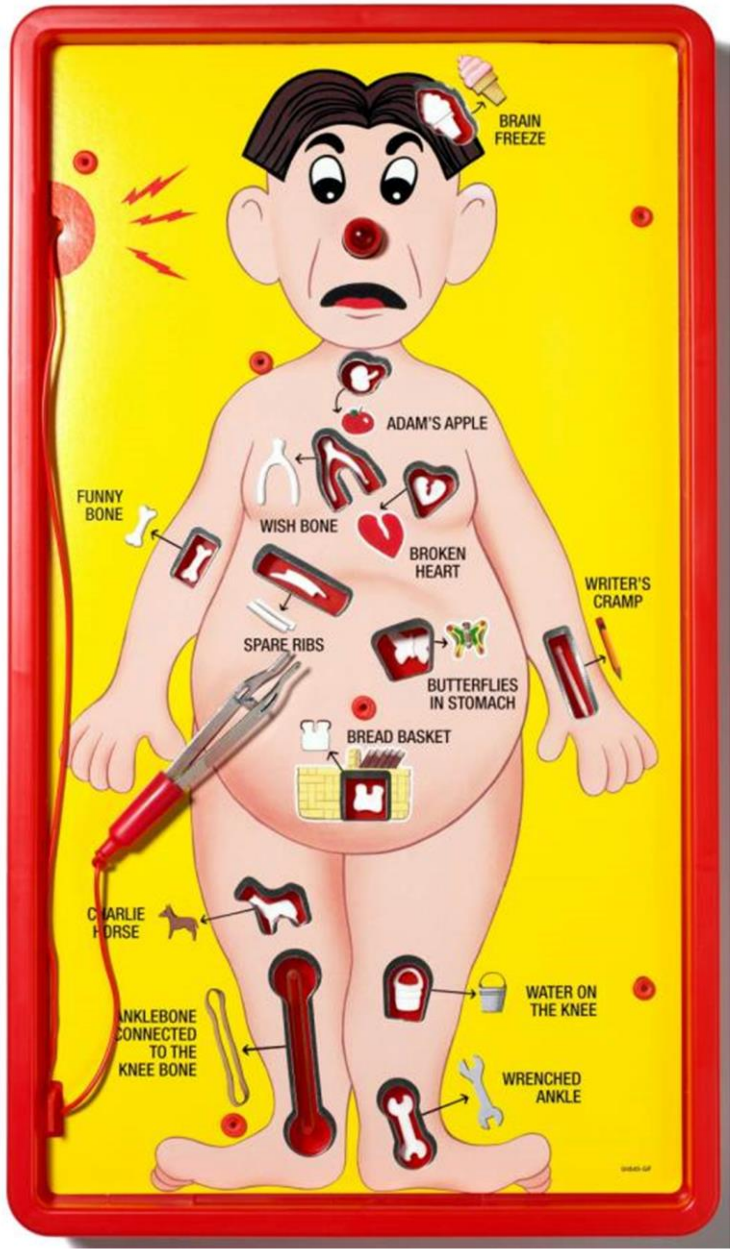
Unique class of industrial IoT
- Remotely configurable
- Bluetooth communications
- GPS tracking

Relatively few devices are designed / manufactured inside the United States

Implanted Medical Devices (IMDs)

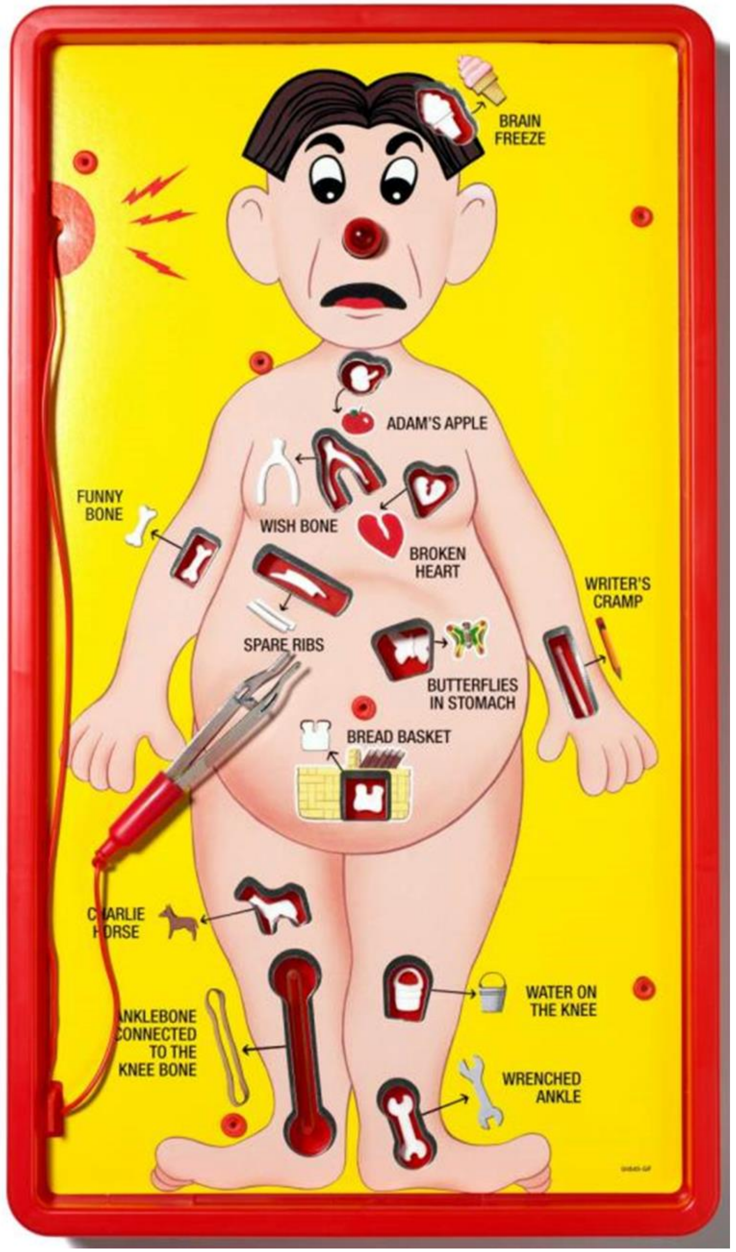


Implanted Medical Devices (IMDs)



WIDEX EVOKE CIC
Micro Smart
Hearing Aid

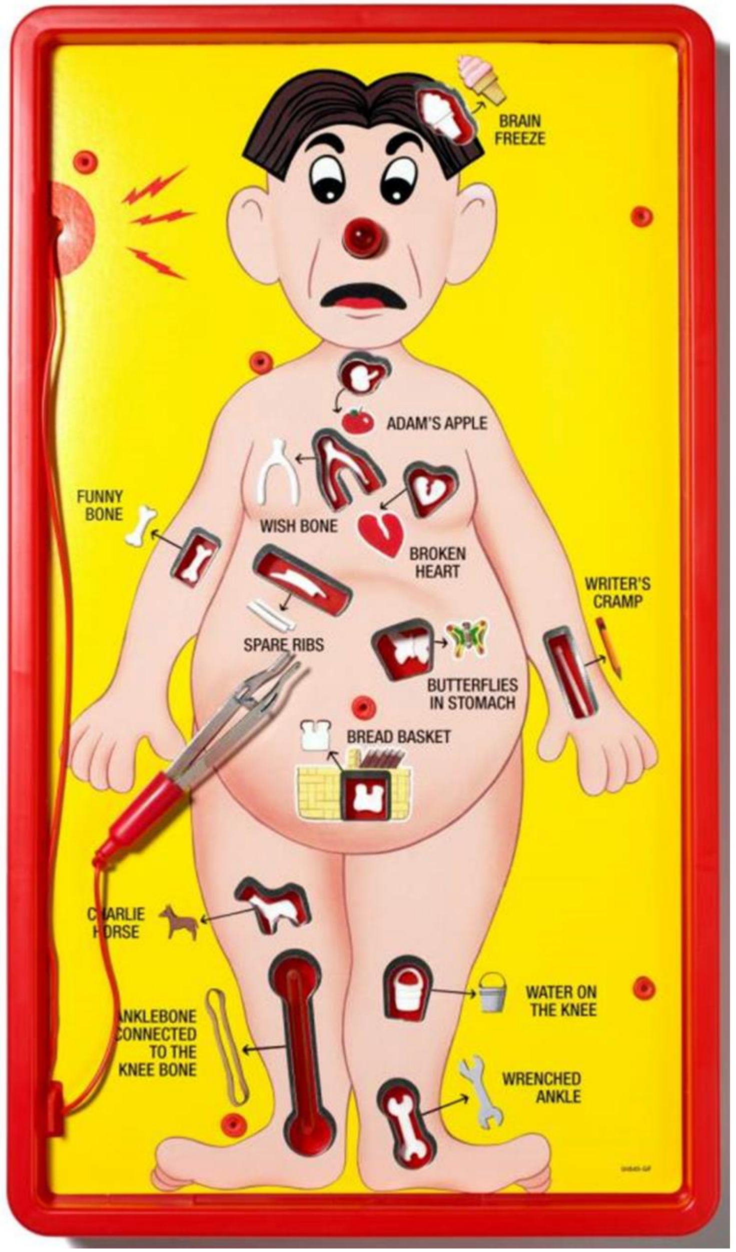
Implanted Medical Devices (IMDs)



WIDEX EVOKE CIC
Micro Smart
Hearing Aid

Automated Device for
Asthma Monitoring and
Management (ADAMM)

Implanted Medical Devices (IMDs)

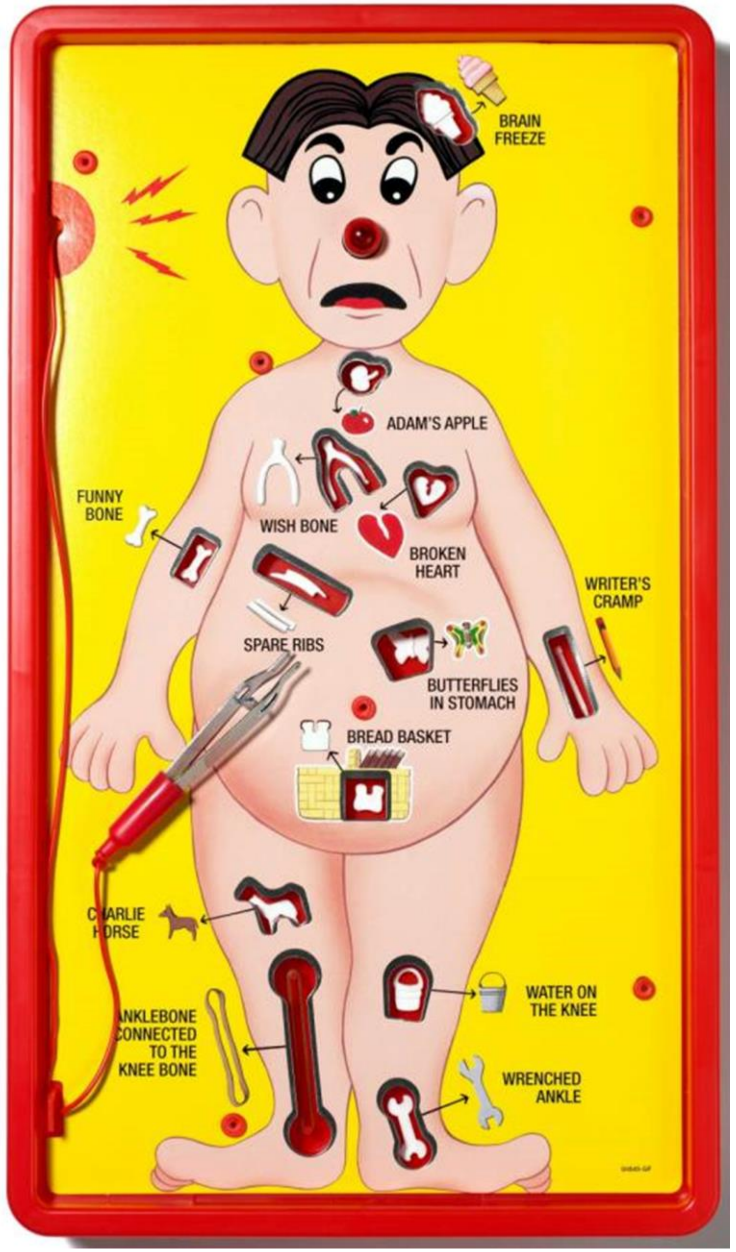


WIDEX EVOKE CIC
Micro Smart
Hearing Aid

Automated Device for
Asthma Monitoring and
Management (ADAMM)

Open Artificial Pancreas System
(OpenAPS) Insulin Pumps

Implanted Medical Devices (IMDs)



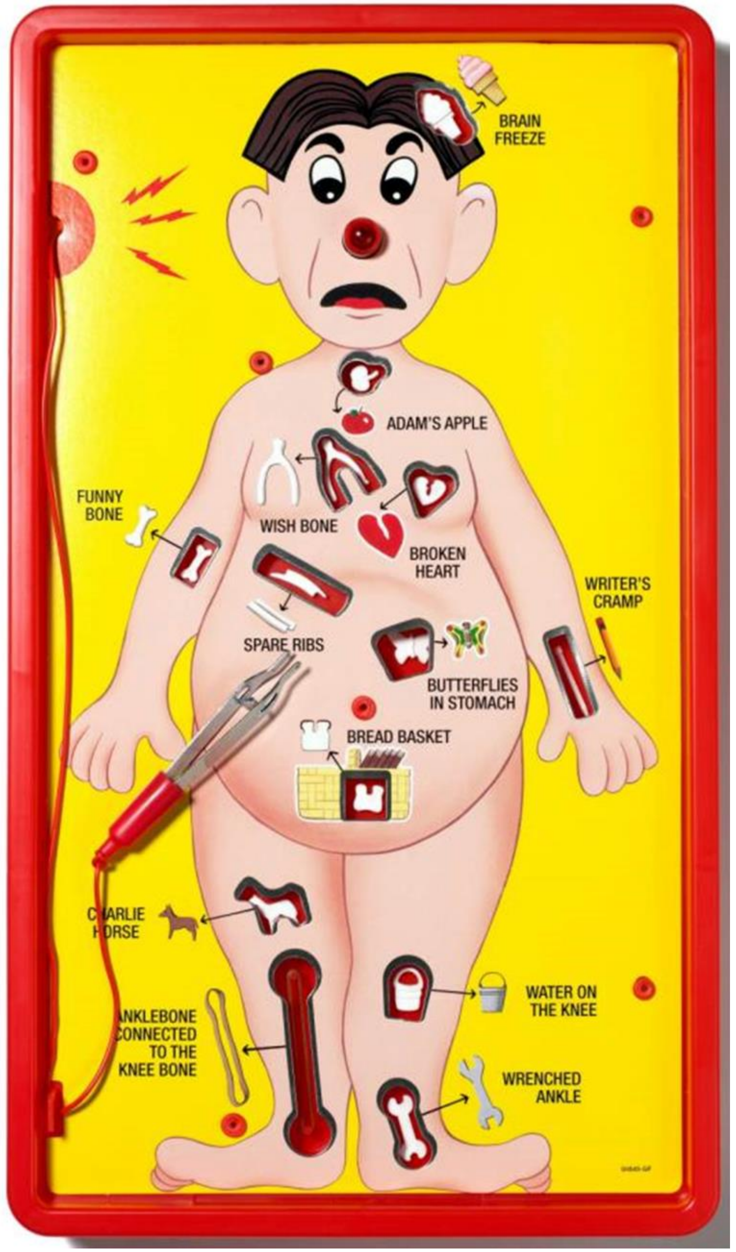
WIDEX EVOKE CIC
Micro Smart
Hearing Aid

Automated Device for
Asthma Monitoring and
Management (ADAMM)

Open Artificial Pancreas System
(OpenAPS) Insulin Pumps

Confirm Rx
Insertable
Cardiac Monitor

Implanted Medical Devices (IMDs)



WIDEX EVOKE CIC
Micro Smart
Hearing Aid

Open Artificial Pancreas System
(OpenAPS) Insulin Pumps

Confirm Rx
Insertable
Cardiac Monitor

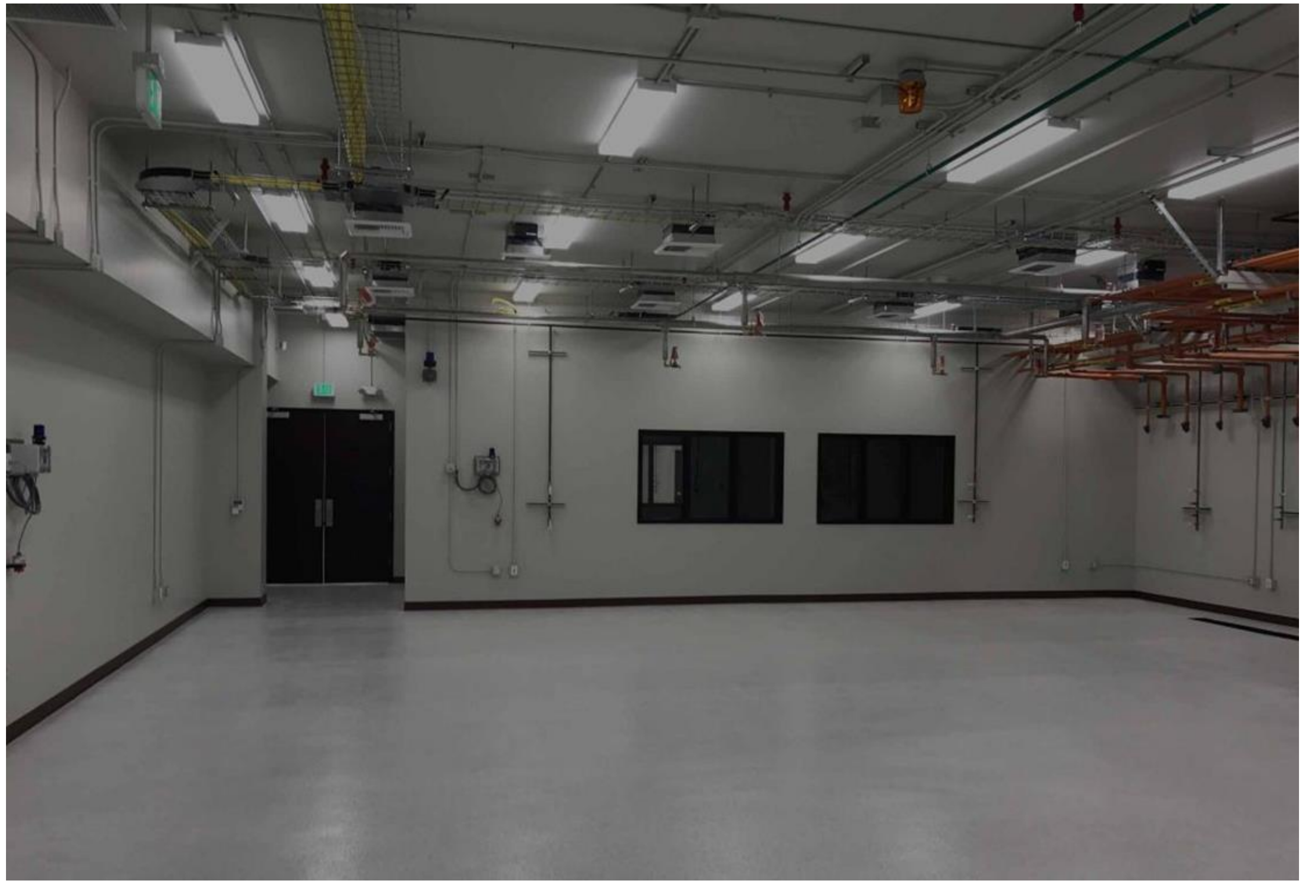
Automated Device for
Asthma Monitoring and
Management (ADAMM)

Azure
Pacemaker

SCIF Requirements*

Physical Security

- Tight perimeter (walls, doors, windows, floors, ceilings)
- Managed penetrations (cables, pipes, HVAC)
- RF shielding for TEMPEST
- Acoustic isolation



Technical Security

- 2a: “**RF transmitters shall not be introduced to a SCIF** unless evaluated and mitigated to be a low risk to classified information by a competent authority…”
- 2b: Restrict access to authorized personnel
- 2c: Intrusion detection systems
- 2e: “**Portable electronic devices pose a risk to SCI** since they often include capabilities to interact with other information systems and can enable hostile attacks targeting classified information in SCIFs.”

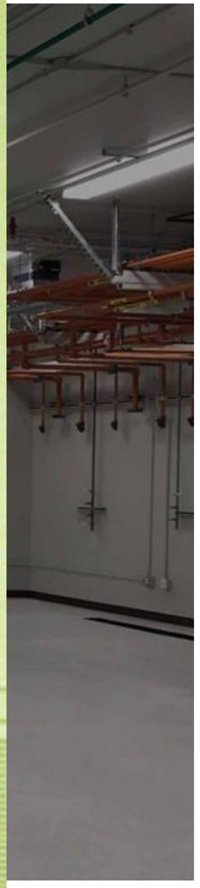
* *Physical and Technical Security Standards for Sensitive Compartmented Information Facilities*, ICS 705-1, 17 Sep 2010
* *Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities*, ICD-705, v1.4

Physic

- Tigh
- Mar
- RF s
- Aco

Techn

- 2a: eva com
- 2b:
- 2c:
- 2e: incl can



* Physical ar
* Technical S

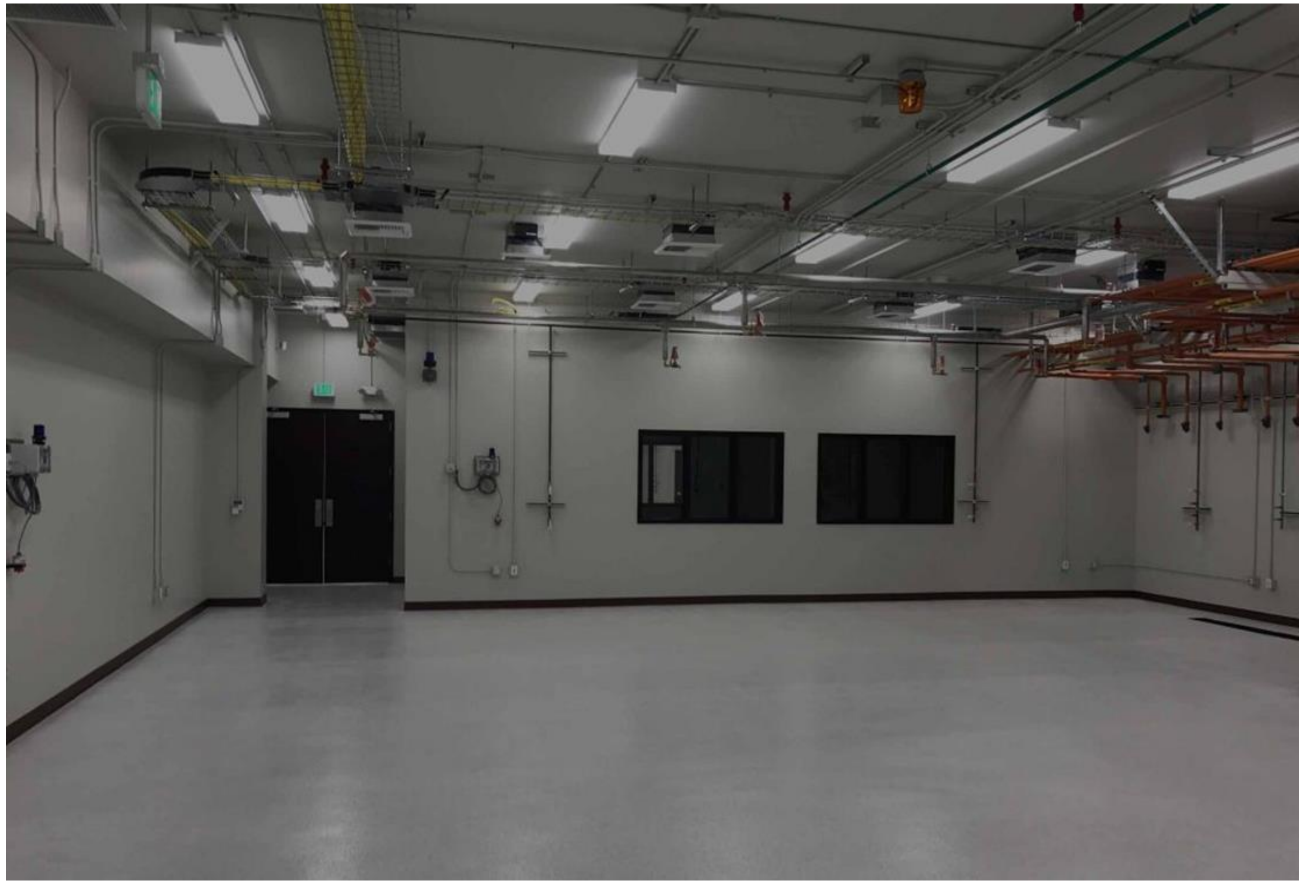
SCIF Requirements*

Physical Security

- Tight perimeter (walls, doors, windows, floors, ceilings)
- Managed penetrations (cables, pipes, HVAC)
- RF shielding for TEMPEST
- Acoustic isolation

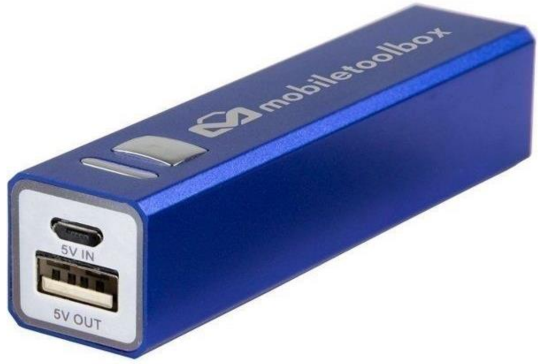
Technical Security

- 2a: "**RF transmitters shall not be introduced to a SCIF** unless evaluated and mitigated to be a low risk to classified information by a competent authority…"
- 2b: Restrict access to authorized personnel
- 2c: Intrusion detection systems
- 2e: "**Portable electronic devices pose a risk to SCI** since they often include capabilities to interact with other information systems and can enable hostile attacks targeting classified information in SCIFs."



* *Physical and Technical Security Standards for Sensitive Compartmented Information Facilities*, ICS 705-1, 17 Sep 2010
* *Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities*, ICD-705, v1.4

Portable Electronic Devices



Portable Electronic Device Risk

Crude guidelines

- Does it have batteries?
- Does it have memory?
- Does it have sensors?
- Can it talk to other devices?
- What benefit does it serve?

PED Risk Levels*

Low-risk PEDs:

- Are without recording or transmission capabilities
- Allowed in without mitigation.

Calculators, RX-only pagers, RX-only radio

Medium-risk PEDs:

- Have built-in features that enable recording or transmitting text, images/video, or audio
- Features can be physically disabled; allowed in with appropriate mitigations.

Dumb phones, airplane mode devices, mics that can be disabled

High-risk PEDs:

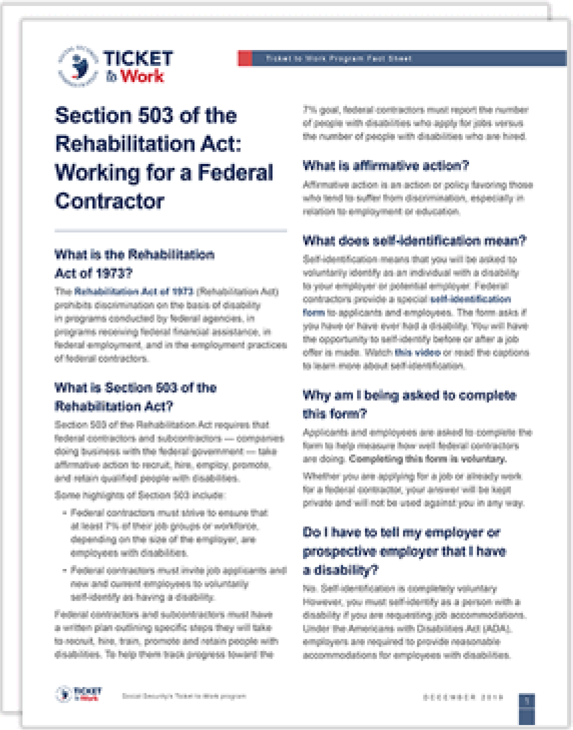
- Have recording and/or transmitting capabilities that cannot be sufficiently mitigated
- May use if mitigation measures reduce the risk to low.

Electronics with RF transmitters (WiFi, Bluetooth, etc), cameras / audio, smart phones

* *Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities*, ICD-705, v1.4

Reasonable Accommodations

Americans with Disabilities Act


TICKET to Work

Ticket to Work Program Fact Sheet

Section 503 of the Rehabilitation Act: Working for a Federal Contractor

What is the Rehabilitation Act of 1973?

The Rehabilitation Act of 1973 (Rehabilitation Act) prohibits discrimination on the basis of disability in programs conducted by federal agencies, in programs receiving federal financial assistance, in federal employment, and in the employment practices of federal contractors.

What is Section 503 of the Rehabilitation Act?

Section 503 of the Rehabilitation Act requires that federal contractors and subcontractors — companies doing business with the federal government — take affirmative action to recruit, hire, employ, promote, and retain qualified people with disabilities.

Some highlights of Section 503 include:

- Federal contractors must strive to ensure that at least 7% of their job groups or workforce, depending on the size of the employer, are employees with disabilities.
- Federal contractors must invite job applicants and new and current employees to voluntarily self-identify as having a disability.

Federal contractors and subcontractors must have a written plan outlining specific steps they will take to recruit, hire, train, promote and retain people with disabilities. To help them track progress toward the 7% goal, federal contractors must report the number of people with disabilities who apply for jobs versus the number of people with disabilities who are hired.

What is affirmative action?

Affirmative action is an action or policy favoring those who tend to suffer from discrimination, especially in relation to employment or education.

What does self-identification mean?

Self-identification means that you will be asked to voluntarily identify as an individual with a disability to your employer or potential employer. Federal contractors provide a special self-identification form to applicants and employees. The form asks if you have or have ever had a disability. You will have the opportunity to self-identify before or after a job offer is made. Watch this video or read the captions to learn more about self-identification.

Why am I being asked to complete this form?

Applicants and employees are asked to complete the form to help measure how well federal contractors are doing. **Completing this form is voluntary.**

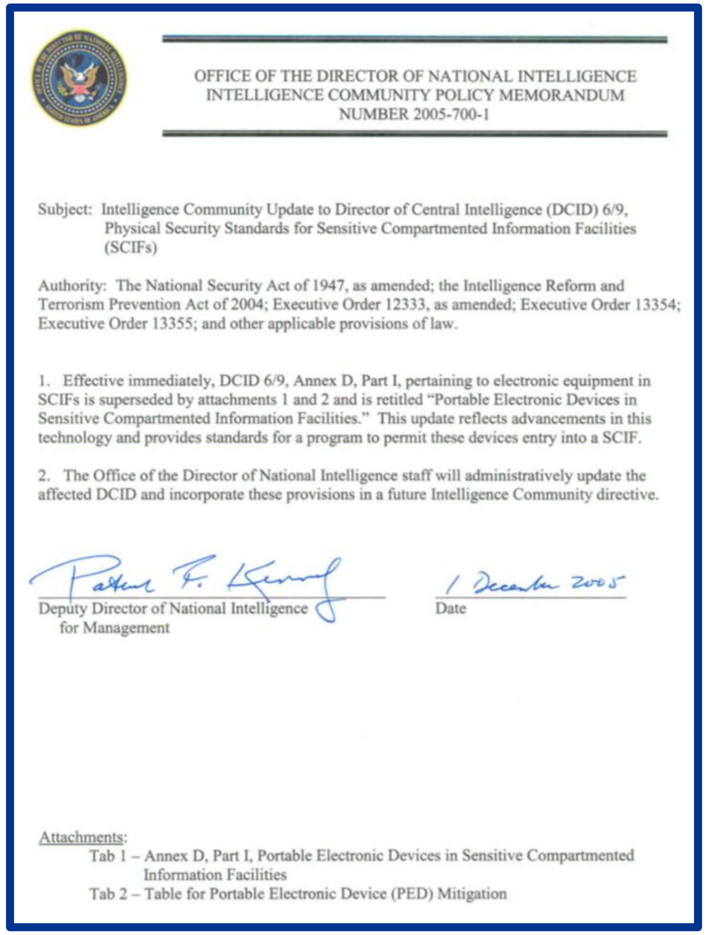
Whether you are applying for a job or already work for a federal contractor, your answer will be kept private and will not be used against you in any way.

Do I have to tell my employer or prospective employer that I have a disability?

No. Self-identification is completely voluntary. However, you must self-identify as a person with a disability if you are requesting job accommodations. Under the Americans with Disabilities Act (ADA), employers are required to provide reasonable accommodations for employees with disabilities.

TICKET to Work Social Security's Ticket to Work program DECEMBER 2019 1

ICPM-2005-700-1*


OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
INTELLIGENCE COMMUNITY POLICY MEMORANDUM
NUMBER 2005-700-1

Subject: Intelligence Community Update to Director of Central Intelligence (DCID) 6/9, Physical Security Standards for Sensitive Compartmented Information Facilities (SCIFs)

Authority: The National Security Act of 1947, as amended; the Intelligence Reform and Terrorism Prevention Act of 2004; Executive Order 12333, as amended; Executive Order 13354; Executive Order 13355; and other applicable provisions of law.

1. Effective immediately, DCID 6/9, Annex D, Part I, pertaining to electronic equipment in SCIFs is superseded by attachments 1 and 2 and is retitled "Portable Electronic Devices in Sensitive Compartmented Information Facilities." This update reflects advancements in this technology and provides standards for a program to permit these devices entry into a SCIF.

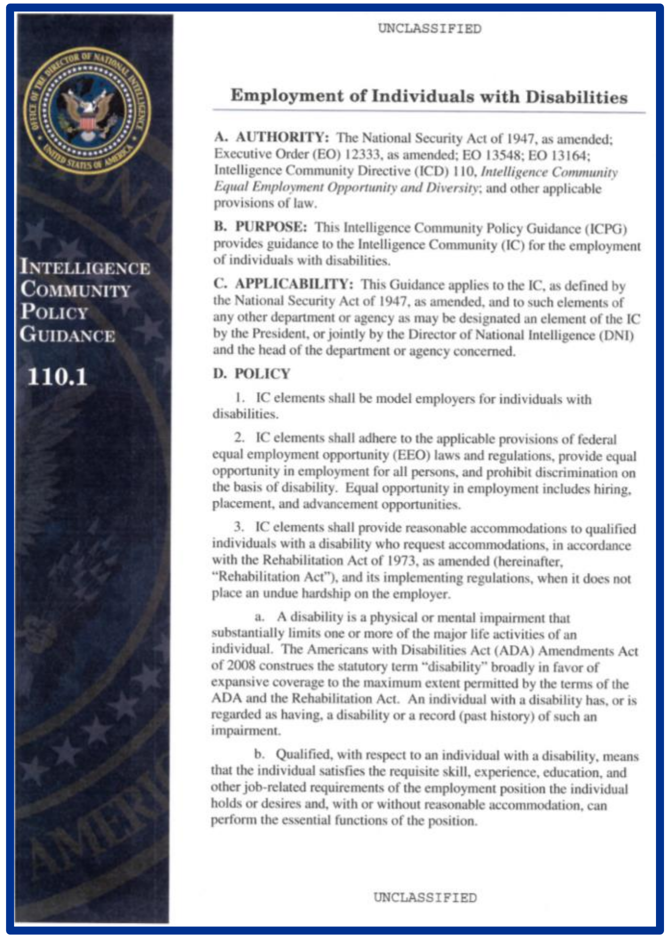
2. The Office of the Director of National Intelligence staff will administratively update the affected DCID and incorporate these provisions in a future Intelligence Community directive.

Patrick F. Kennedy
Deputy Director of National Intelligence for Management

1 December 2005
Date

Attachments:
Tab 1 – Annex D, Part I, Portable Electronic Devices in Sensitive Compartmented Information Facilities
Tab 2 – Table for Portable Electronic Device (PED) Mitigation

ICPG-110.1 (2009)


INTELLIGENCE COMMUNITY POLICY GUIDANCE 110.1

UNCLASSIFIED

Employment of Individuals with Disabilities

A. **AUTHORITY:** The National Security Act of 1947, as amended; Executive Order (EO) 12333, as amended; EO 13548; EO 13164; Intelligence Community Directive (ICD) 110, *Intelligence Community Equal Employment Opportunity and Diversity*; and other applicable provisions of law.

B. **PURPOSE:** This Intelligence Community Policy Guidance (ICPG) provides guidance to the Intelligence Community (IC) for the employment of individuals with disabilities.

C. **APPLICABILITY:** This Guidance applies to the IC, as defined by the National Security Act of 1947, as amended, and to such elements of any other department or agency as may be designated an element of the IC by the President, or jointly by the Director of National Intelligence (DNI) and the head of the department or agency concerned.

D. **POLICY**

1. IC elements shall be model employers for individuals with disabilities.

2. IC elements shall adhere to the applicable provisions of federal equal employment opportunity (EEO) laws and regulations, provide equal opportunity in employment for all persons, and prohibit discrimination on the basis of disability. Equal opportunity in employment includes hiring, placement, and advancement opportunities.

3. IC elements shall provide reasonable accommodations to qualified individuals with a disability who request accommodations, in accordance with the Rehabilitation Act of 1973, as amended (hereinafter, "Rehabilitation Act"), and its implementing regulations, when it does not place an undue hardship on the employer.

a. A disability is a physical or mental impairment that substantially limits one or more of the major life activities of an individual. The Americans with Disabilities Act (ADA) Amendments Act of 2008 construes the statutory term "disability" broadly in favor of expansive coverage to the maximum extent permitted by the terms of the ADA and the Rehabilitation Act. An individual with a disability has, or is regarded as having, a disability or a record (past history) of such an impairment.

b. Qualified, with respect to an individual with a disability, means that the individual satisfies the requisite skill, experience, education, and other job-related requirements of the employment position the individual holds or desires and, with or without reasonable accommodation, can perform the essential functions of the position.

UNCLASSIFIED

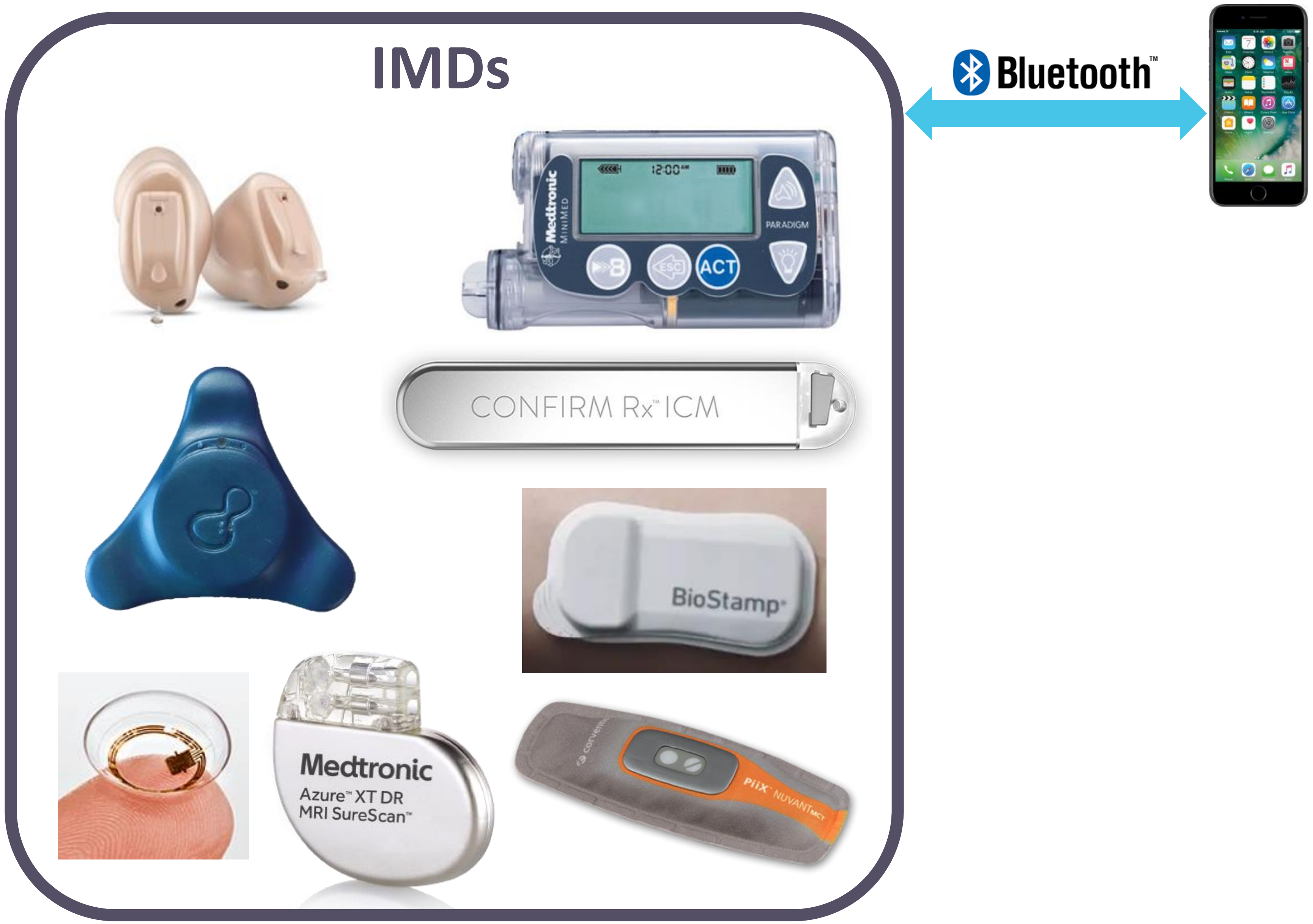
EO 13163 (7/2000)
EO 13518 (11/2009)
EO 13548 (7/2010)

* *Superceded by* ICD-705, v1.2/v1.3/v1.4

Risks Associated with IMDs

IMDs

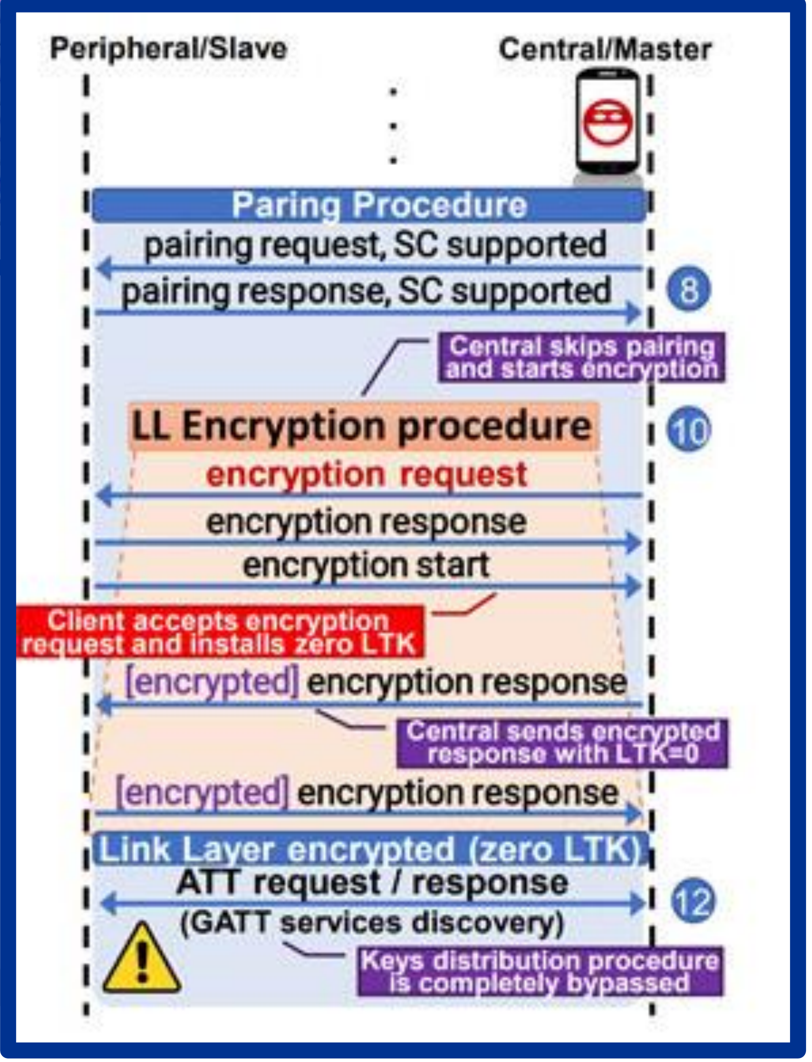
Risks Associated with IMDs



black hat USA 2020

Type	Vulnerability Name	Affected Vendors	CVE
Crash	Link Layer Length Overflow	Cypress NXP	CVE-2019-16336 (6.1) CVE-2019-17519 (6.1)
	Truncated L2CAP	Dialog Semiconductors	CVE-2019-17517 (6.3)
	Silent Length Overflow	Dialog Semiconductors	CVE-2019-17518 (6.4)
	Public Key Crash	Texas Instruments	CVE-2019-17520 (6.6)
	Invalid L2CAP Fragment	Microchip	CVE-2019-19195 (6.8)
	Key Size Overflow	Telink Semiconductor	CVE-2019-19196 (6.9)
Deadlock	LLID Deadlock	Cypress NXP	CVE-2019-17061 (6.2) CVE-
	Sequential ATT Deadlock	STMicroelectronics	CVE-
	Invalid Connection Request	Texas Instruments	CVE-
Security Bypass	Zero LTK Installation	Telink Semiconductor	CVE-2

SWEYNTOOTH



Risks Associated with IMDs

Risks Associated with IMDs

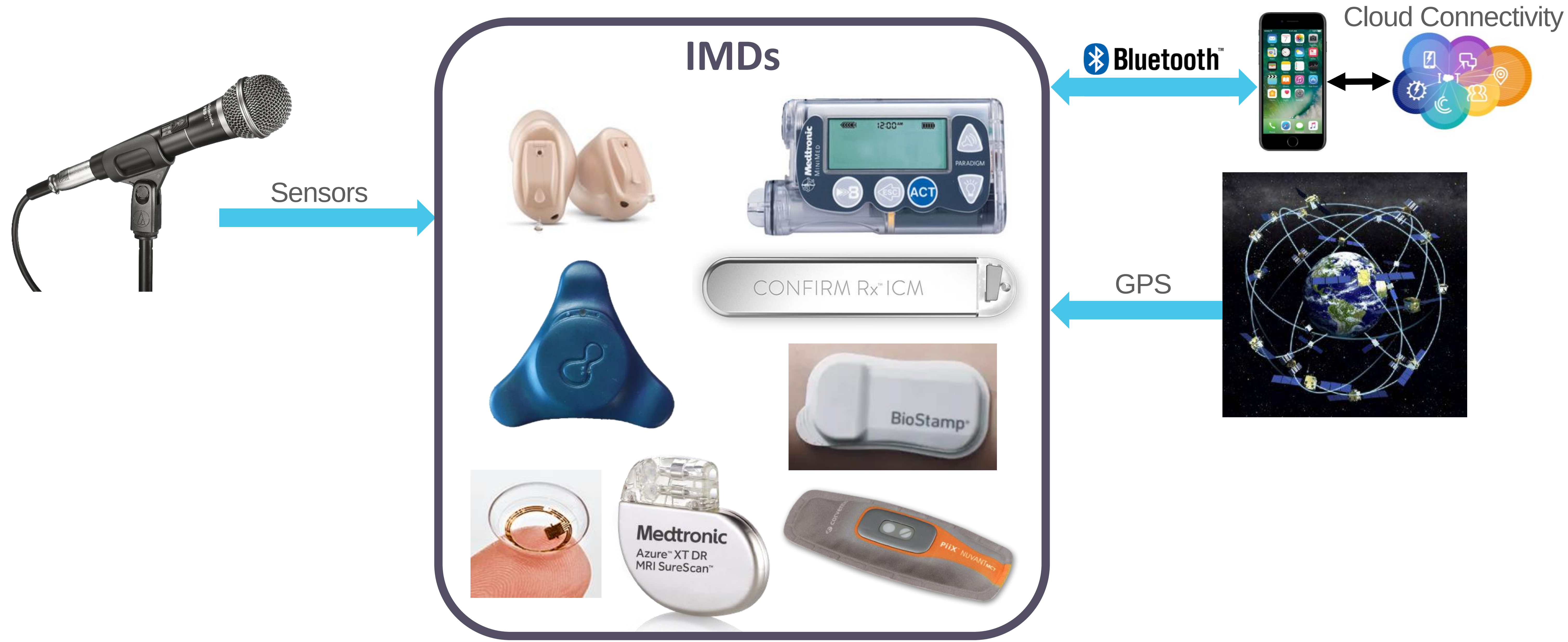
Sensors

IMDs

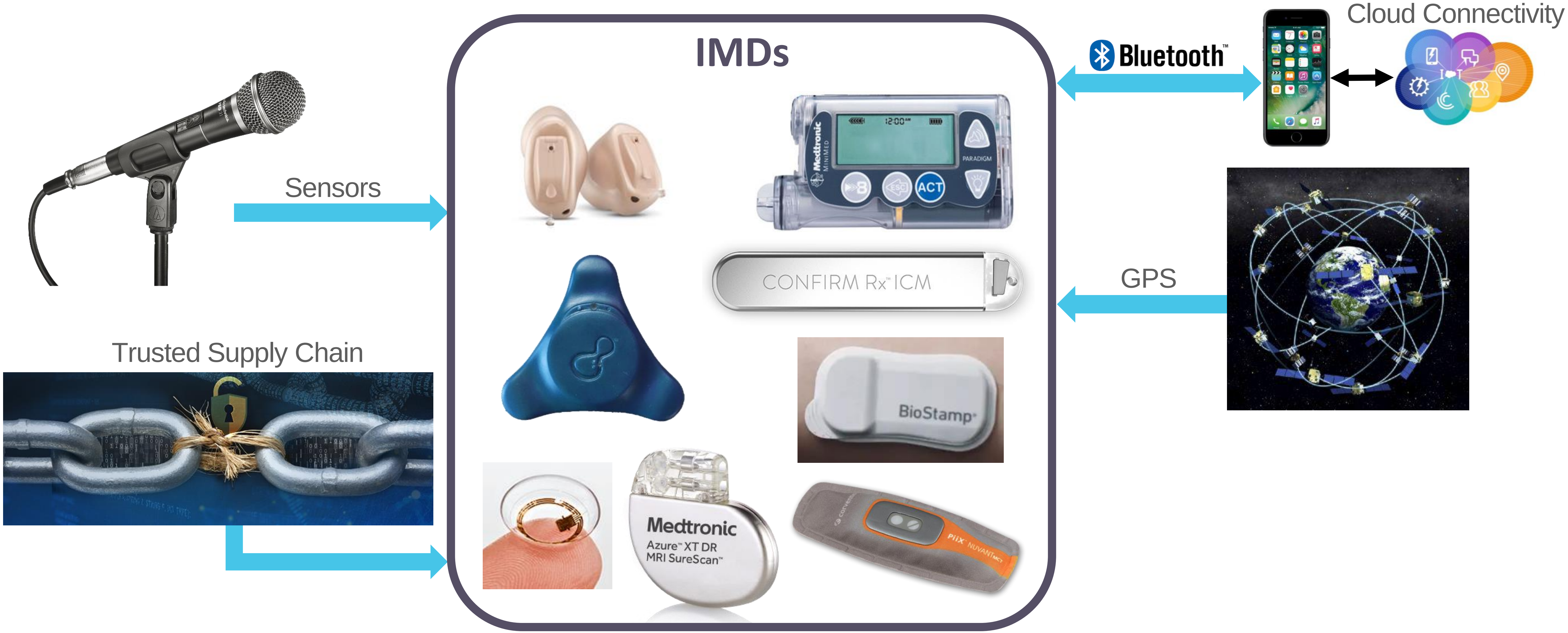
Bluetooth

Cloud Connectivity

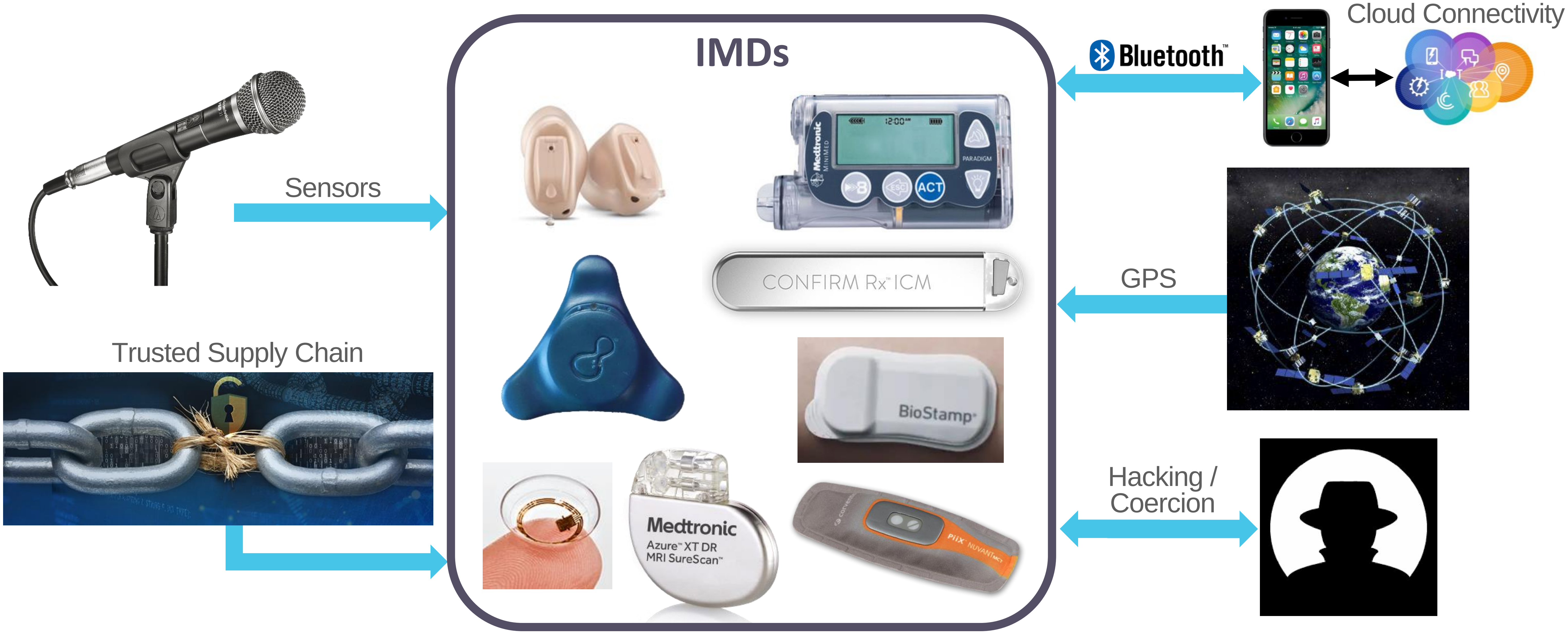
Risks Associated with IMDs



Risks Associated with IMDs



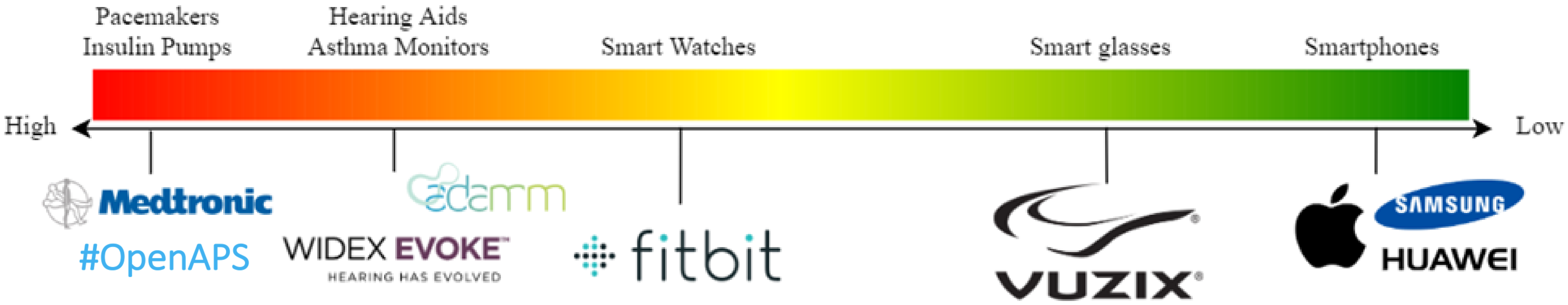
Risks Associated with IMDs



PED Risk after current Mitigations

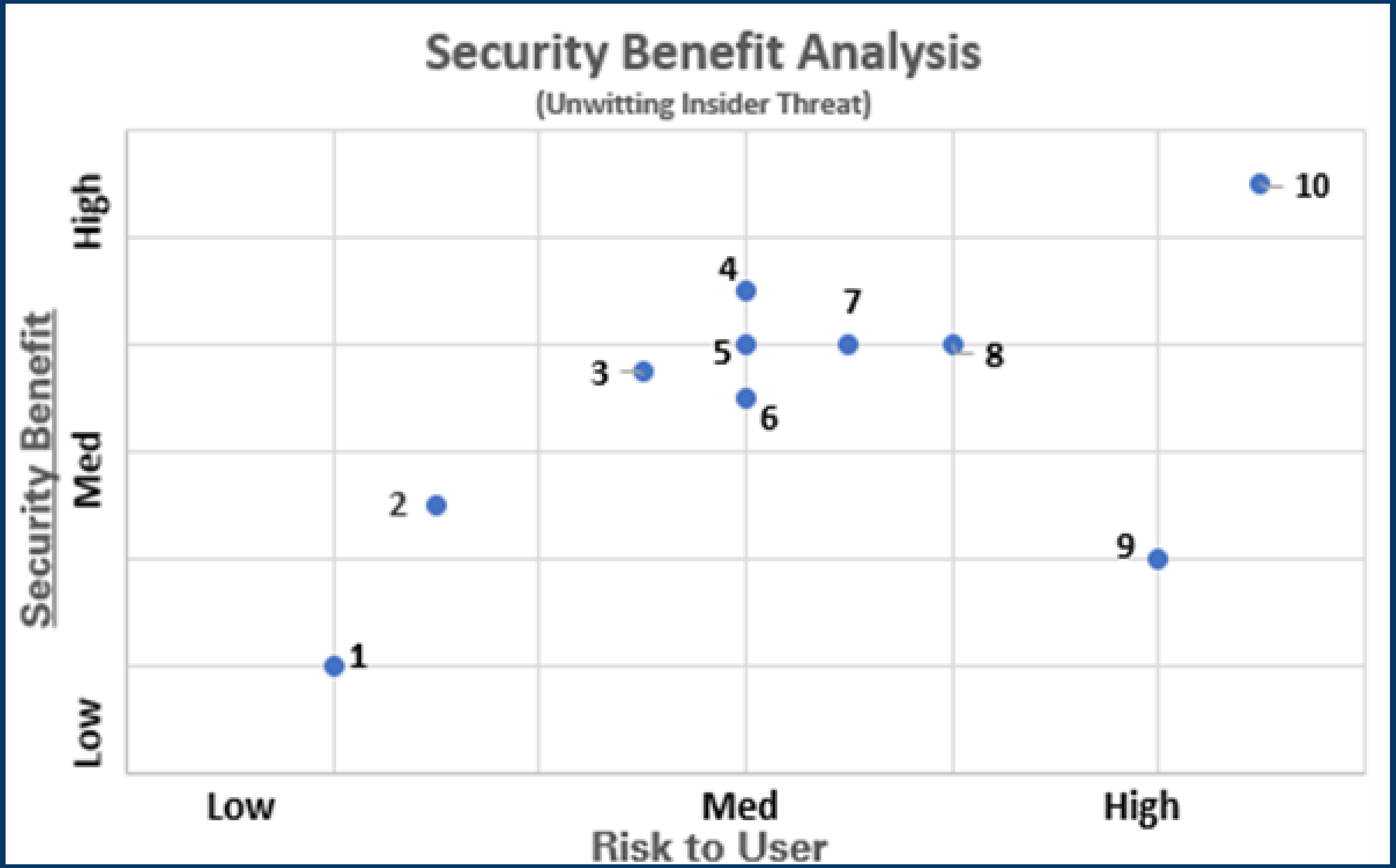
ICD-705 Guidance on Medical Devices (Chapter 10)

- **v1.2, 4/2012:** N/A
- **v1.3, 9/2015:** Footnote: *Medical devices are exceptions to these requirements*.
- **v1.4, 9/2017:** (Paragraph 3) *Approval for medical devices will comply with all applicable laws and oversight policies, including the Rehabilitation Act, and the latest IC medical device approval process. As a minimum, the medical device must be reviewed to determine any technical security issues introduced by the device. Based on the security/technical review, medical devices may be approved by the Accrediting Official for introduction and use within a SCIF.*
- **Now, 2020:**

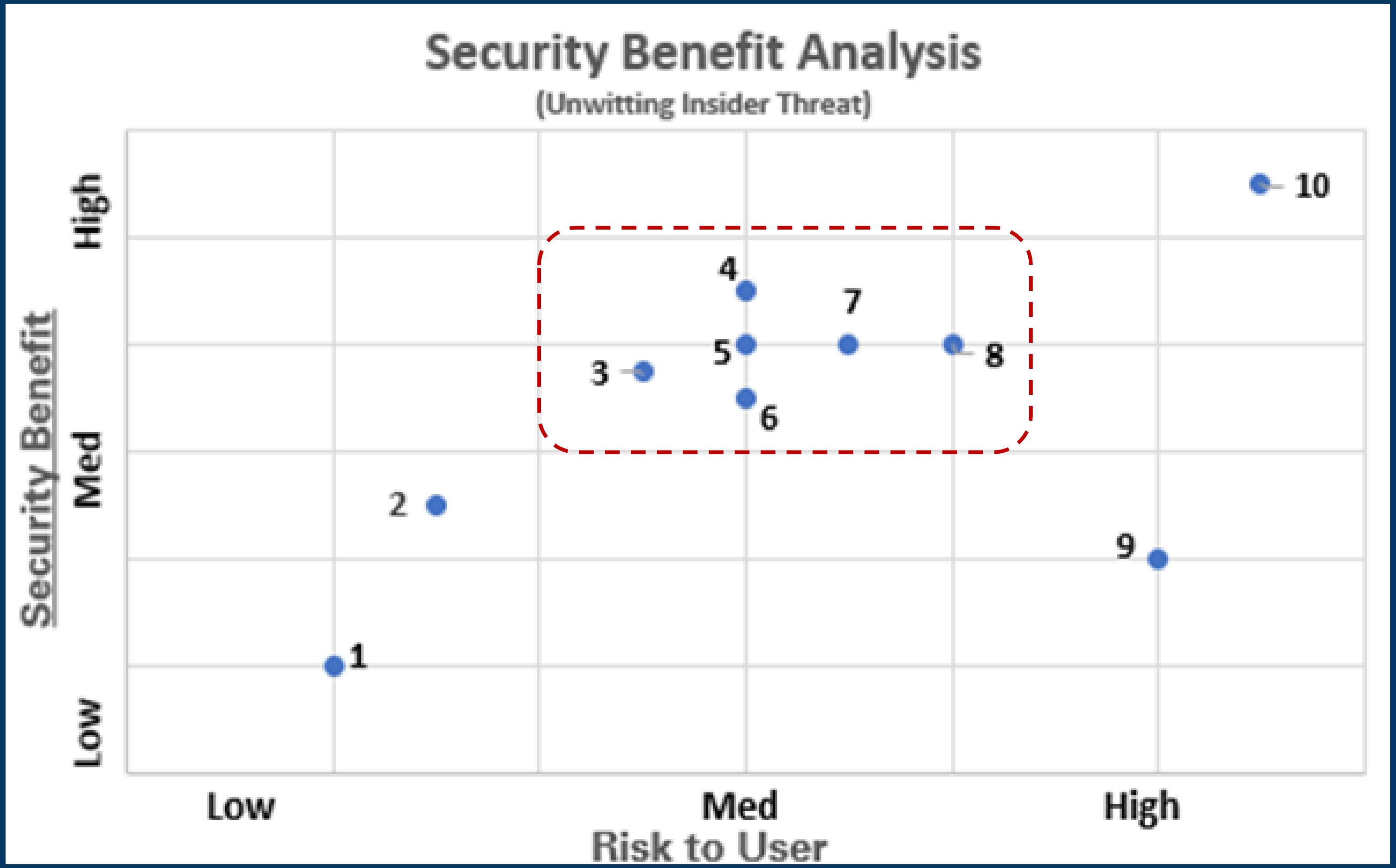


* *Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities*, ICD-705, v1.2/v1.3/v1.4

Proposed Mitigations

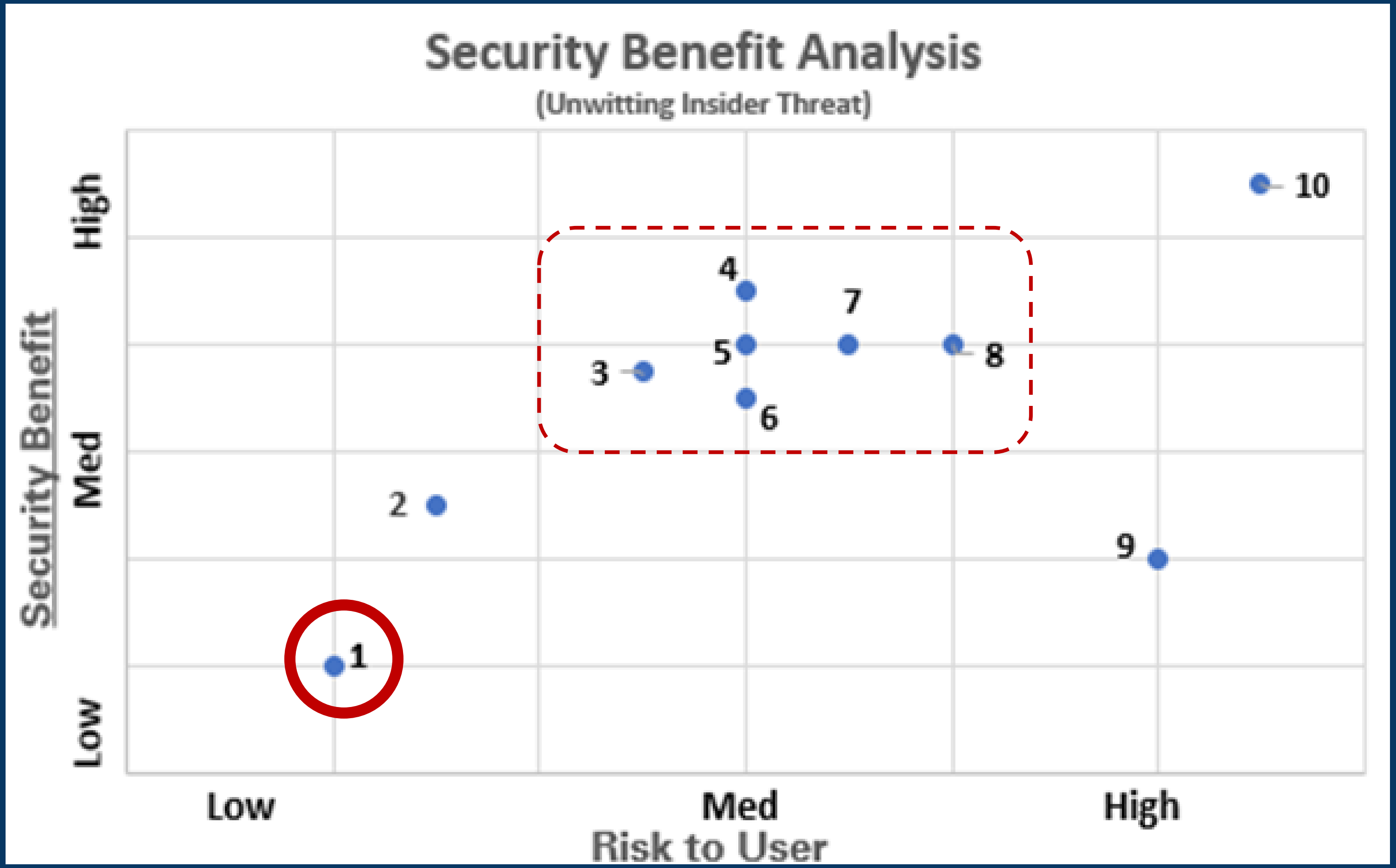


Proposed Mitigations



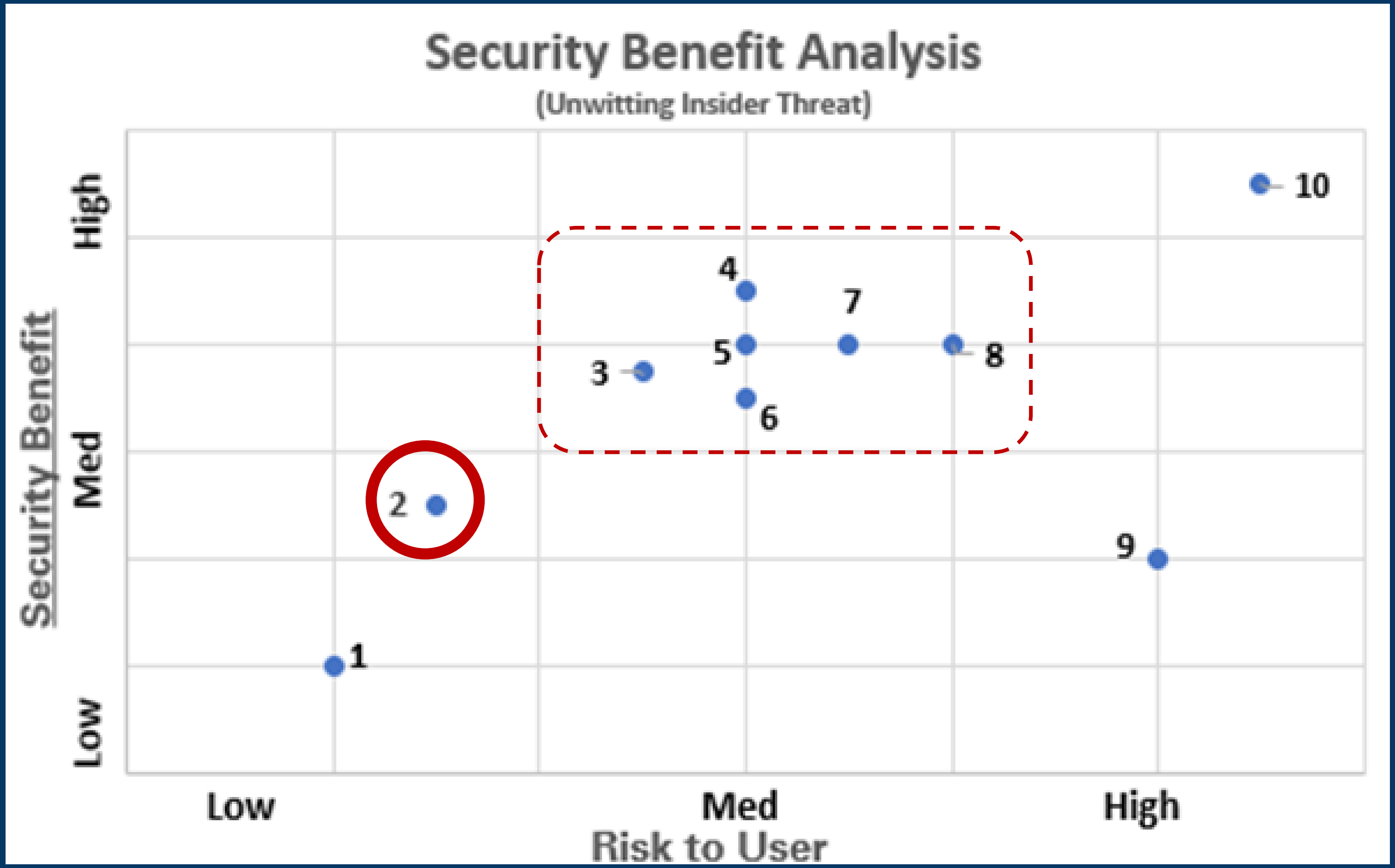
Proposed Mitigations

(1) Random Physical Inspections



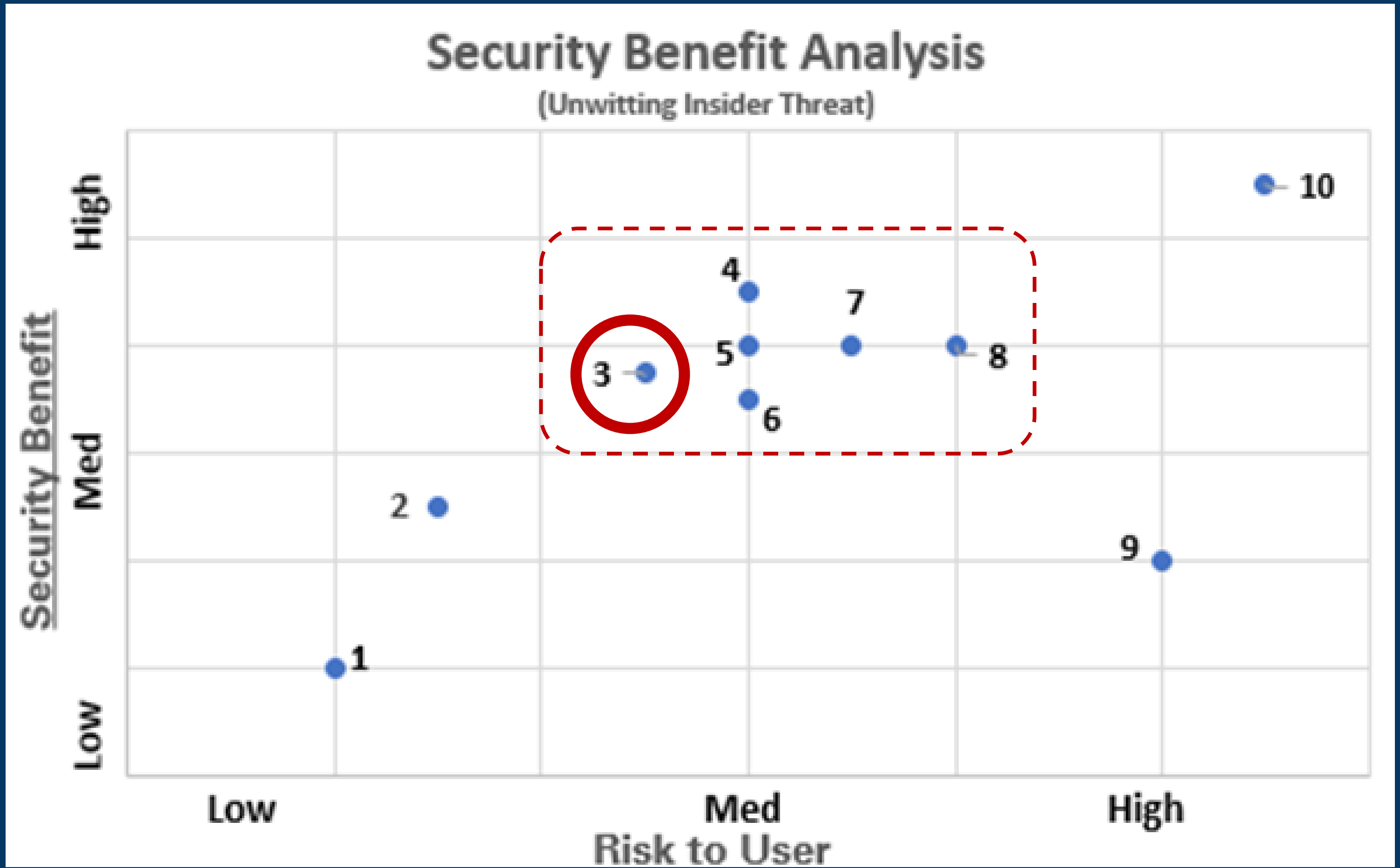
Proposed Mitigations

(2) Ferromagnetic Detection Systems



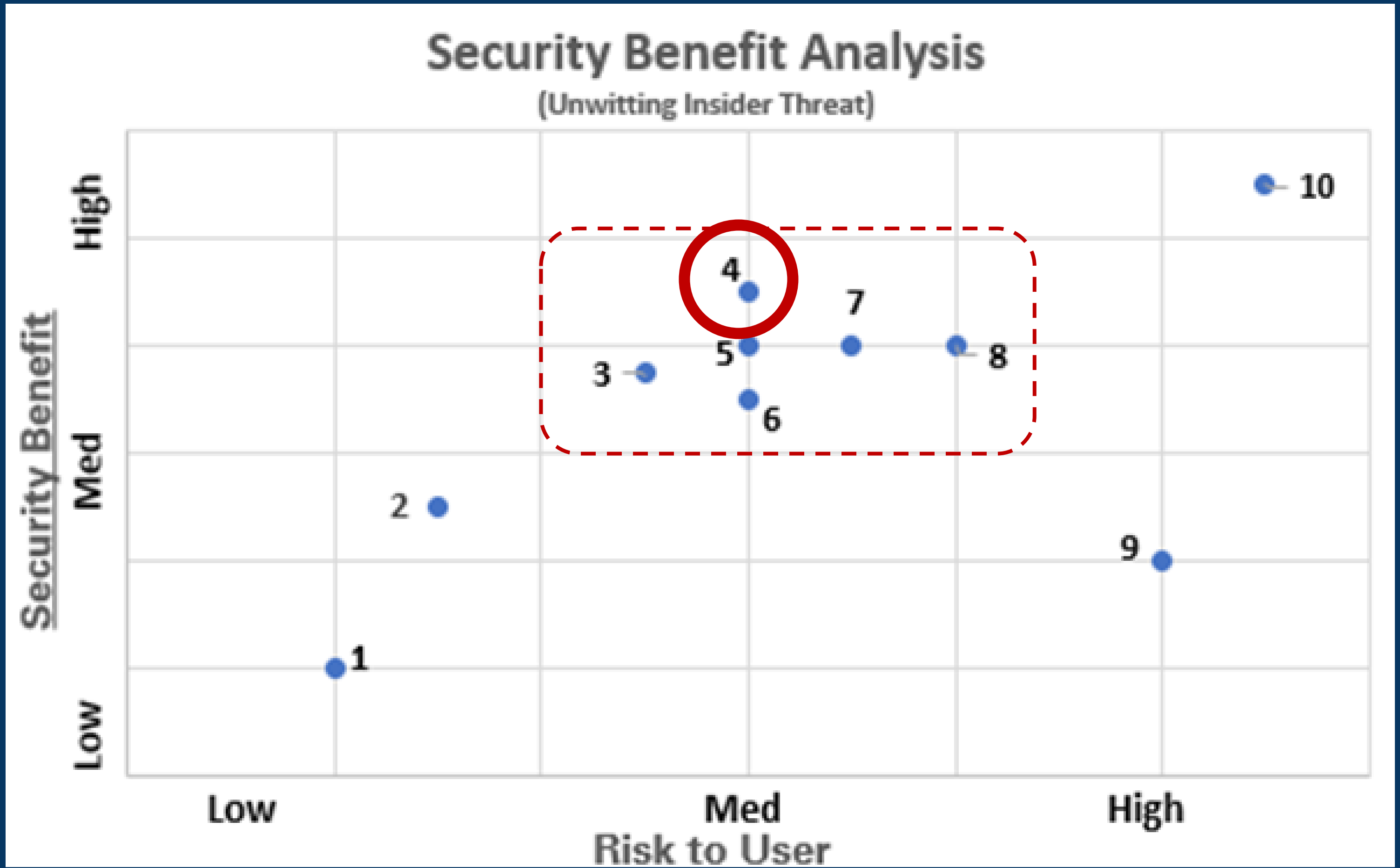
Proposed Mitigations

(3) RF Shielding Apparel



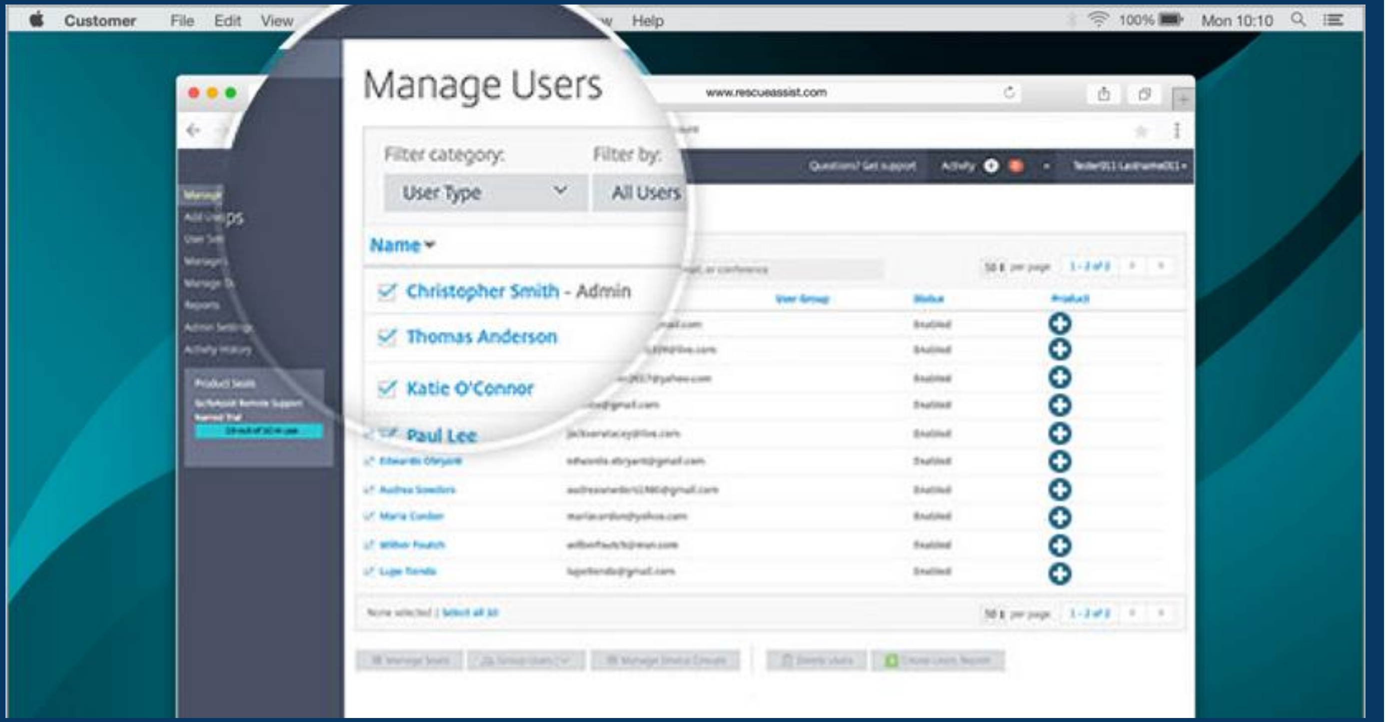
Proposed Mitigations

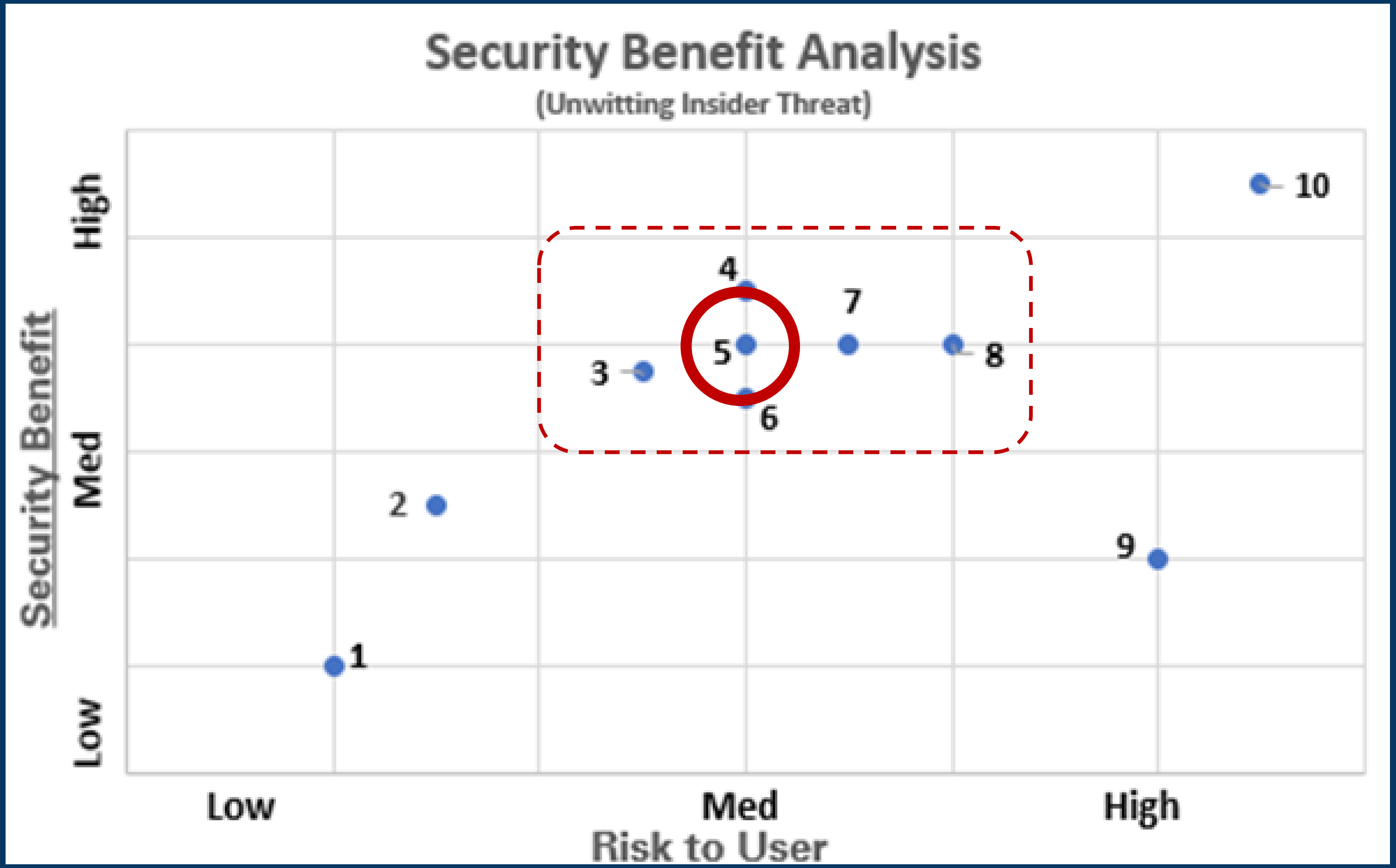
(4) Zeroization



Proposed Mitigations

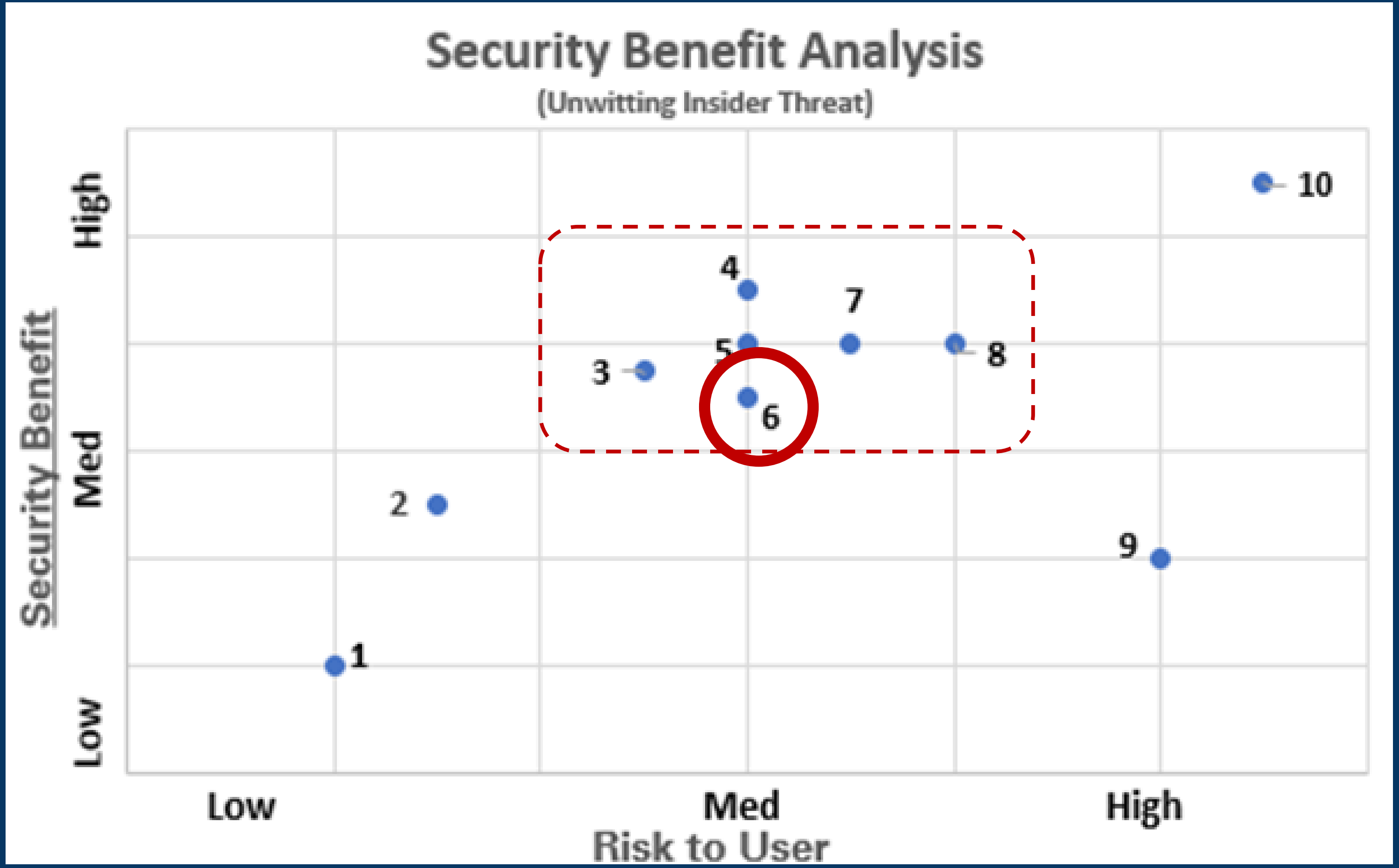
(5) Password Activated Software





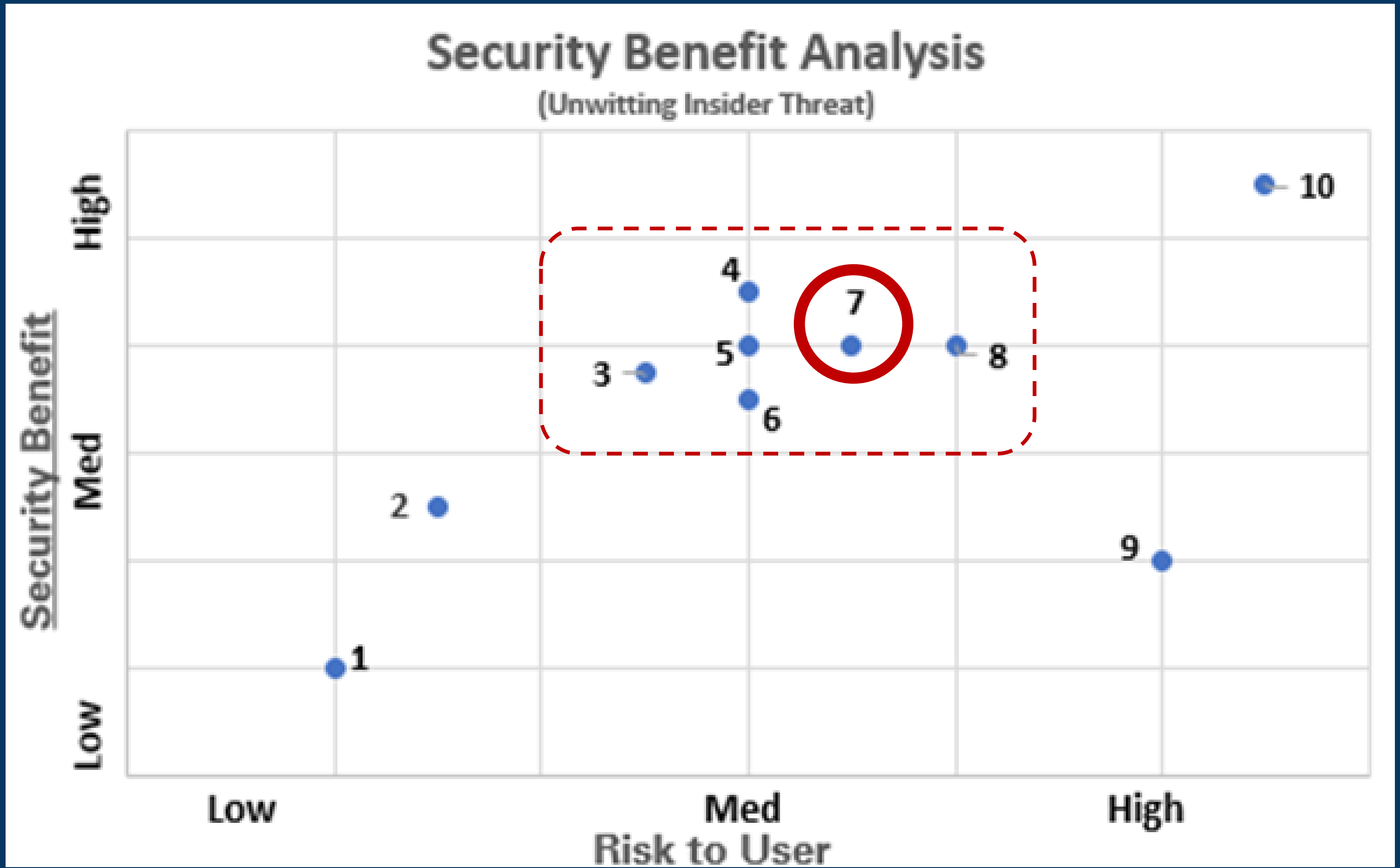
Proposed Mitigations

(6) Temporarily Muting Transducers



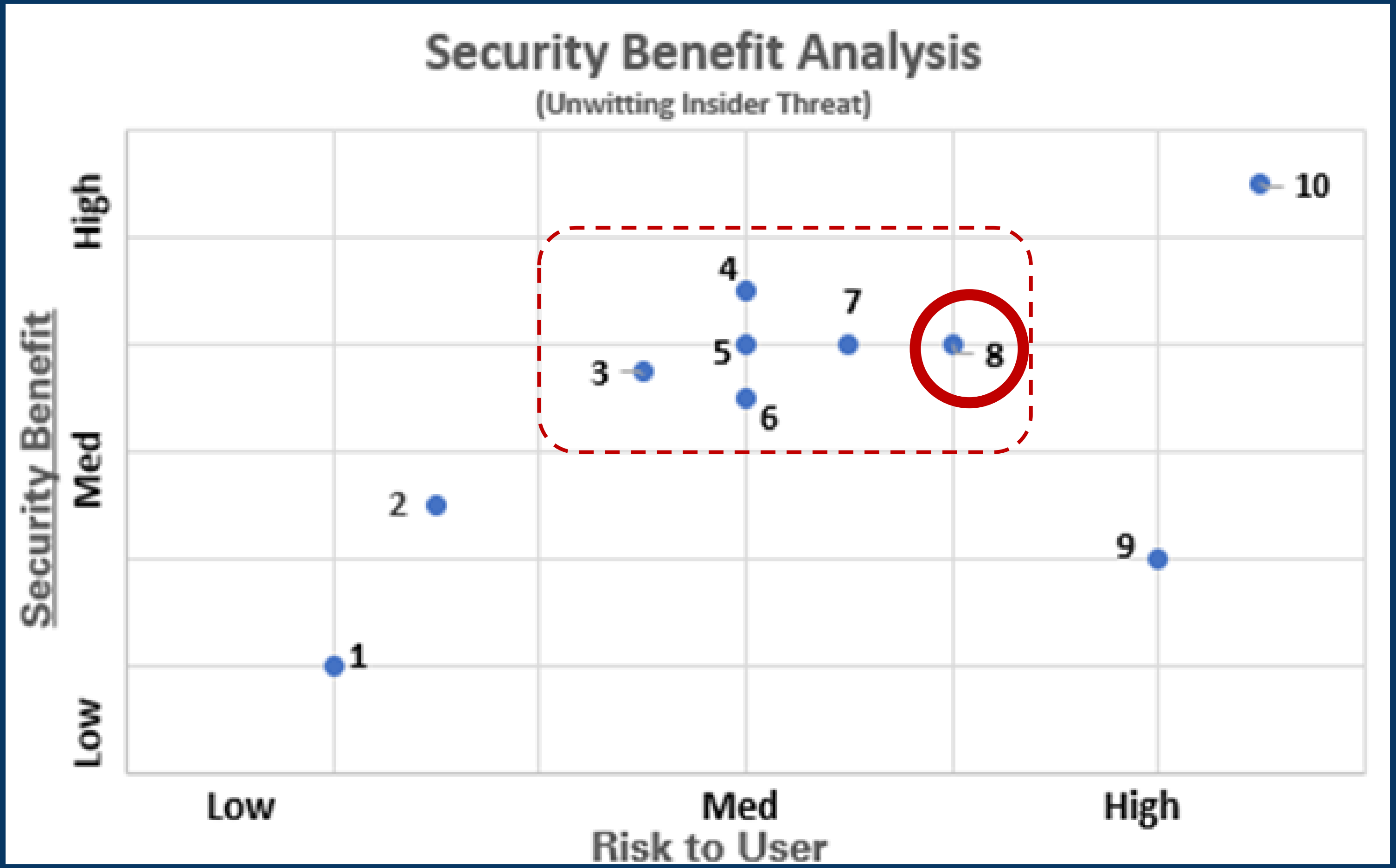
Proposed Mitigations

(7) Personal Jamming



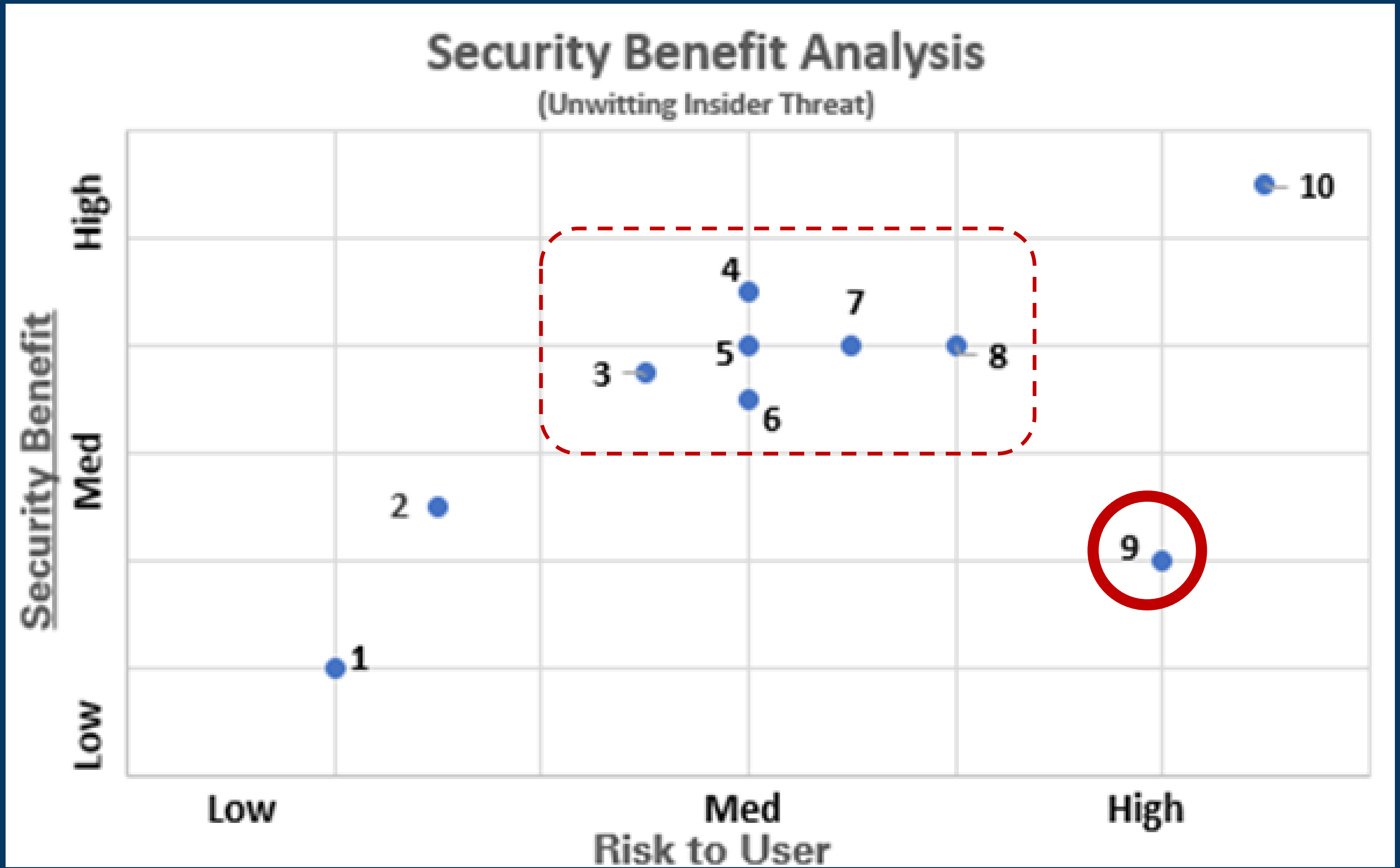
Proposed Mitigations

(8) General Signal Jamming/AP Spoofing



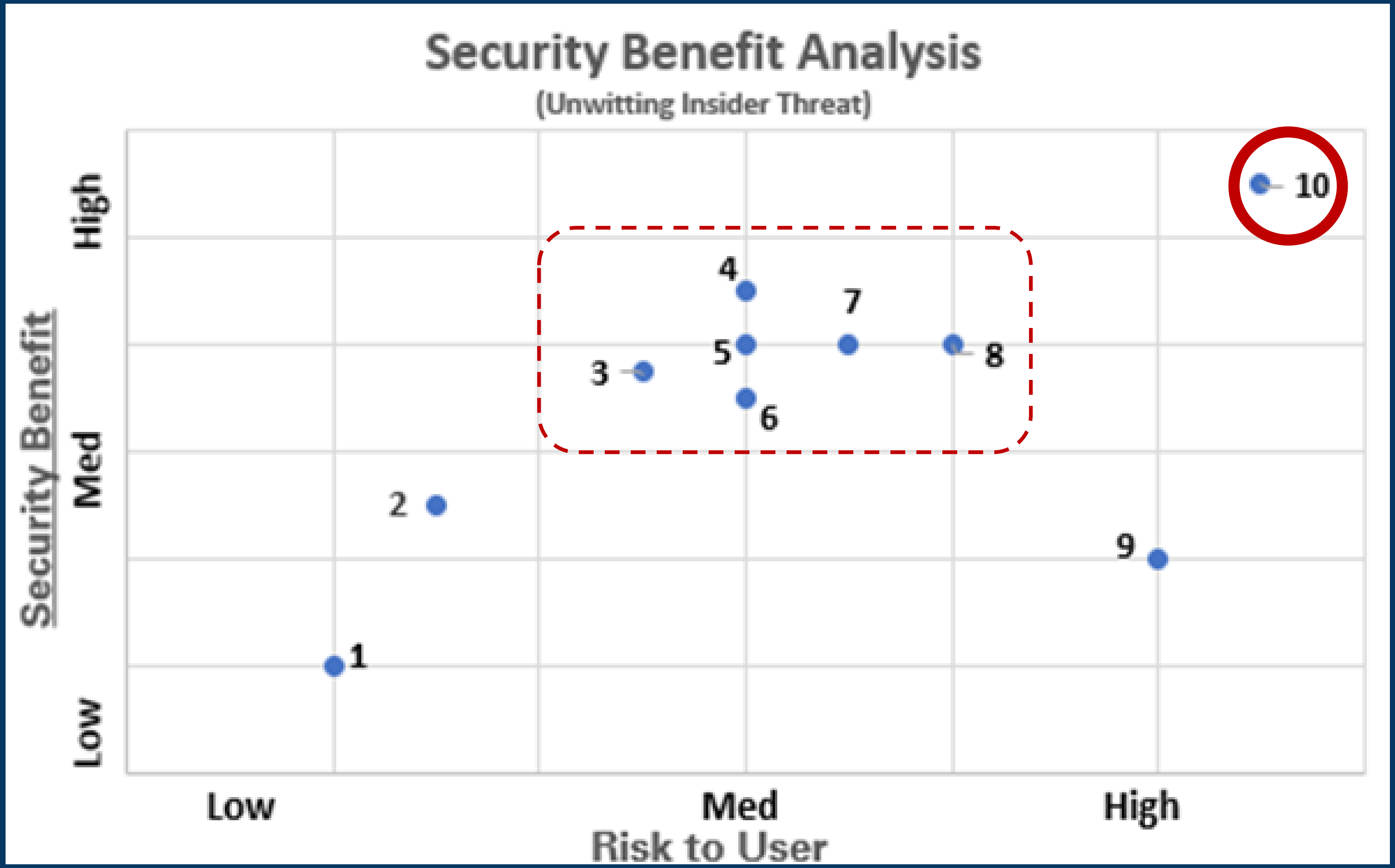
Proposed Mitigations

(9) Tracking/RF Fingerprint technologies



Proposed Mitigations

(10) Denying Entry



Proposed Mitigations

(1) Random Physical Inspections

(2) Ferromagnetic Detection Systems

(3) RF Shielding Apparel

(4) Zeroization

(5) Password Activated Software

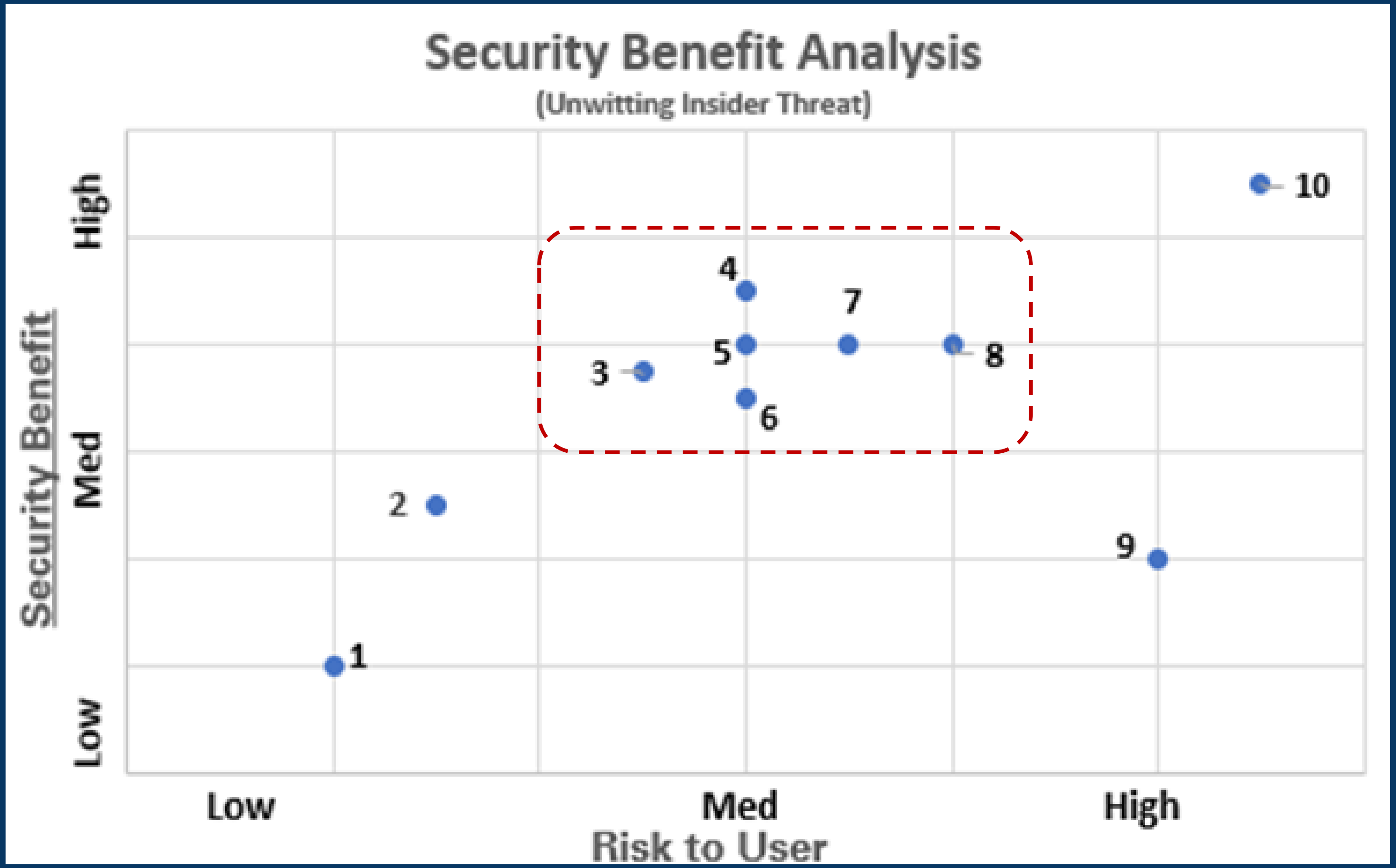
(6) Temporarily Muting Transducers

(7) Personal Jamming

(8) General Signal Jamming/AP Spoofing

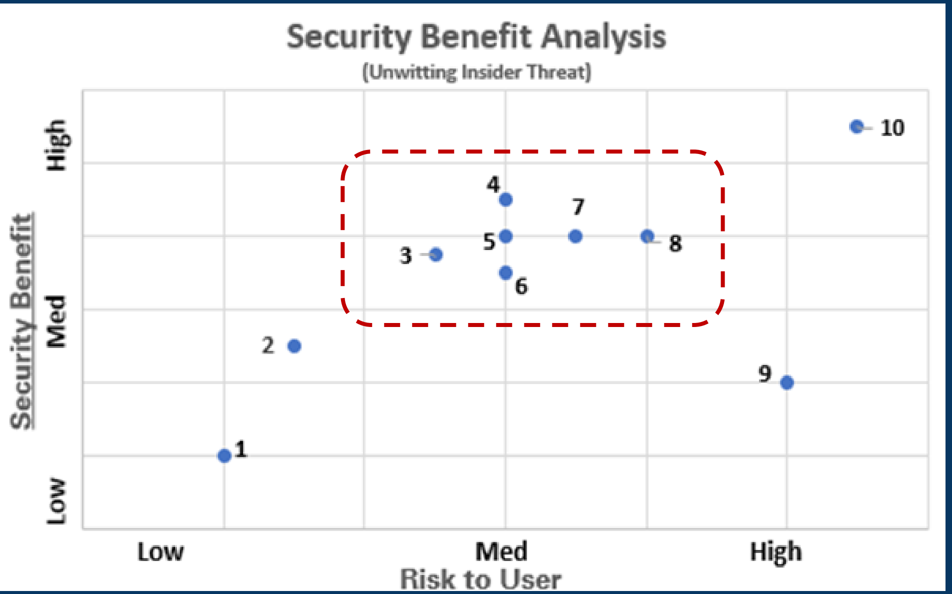
(9) Tracking/RF Fingerprint technologies

(10) Denying Entry



Proposed Mitigations

- ***(1) Random Physical Inspections*** are similar to ICD-705 policy on government provided devices. Poses a low risk to the user; however, without sufficient knowledge on the specific device, difficult to catch the unauthorized extraction of data.
- ***(2) Ferromagnetic Detection Systems*** may help identify smart devices before they enter any secure area, leading to facility manager decision whether or not to admit the individual. These systems do not prevent data extraction, only the detection of the physical device.
- ***(3) RF Shielding Apparel*** could be a foil vest that blocks communication with the IMD. This proposed vest would be worn by the host upon entering the facility. Signal leakage is still a concern.
- ***(4) Zeroization*** is a safe method, but requires knowledge of the device and settings. All sensor data collected inside the SCIF must be removed to ensure protections. Because of this, a greater risk is imposed upon the user, because stored settings or essential functions may be disrupted.
- ***(5) Password Activated Software*** is an administrator controlled software that takes over control of the device and limits suspect functions until a password is entered. This one-time use password would be provided to the employee after they have left the secure area.
- ***(6) Temporarily Muting Transducers*** ensures valuable data cannot be recorded and stored. Users with cochlear implants would lose functionality as well as other similar styles of implants, many of whose residual capabilities impair human health.



- ***(7) Personal Jamming*** actively impairs the communication or sensor functions, much like an audio white noise generator.
- ***(8) General Signal Jamming/AP Spoofing*** hijacks Bluetooth, WiFi, and other commercial signals, preventing communication to third parties. This proves beneficial as no privacy laws are violated, yet could result in battery draws or other unintended effects to the medical device.
- ***(9) Tracking/RF Fingerprint technologies*** mark an individual and monitor location and possibly record any signals. Such a technique likely violates privacy/HIPAA laws.
- ***(10) Denying Entry*** completely eliminates the risk of data extraction, however the user would not be permitted to conduct any work within the area. While denial provides security, it fails to meet the practical needs of our ageing workforce.

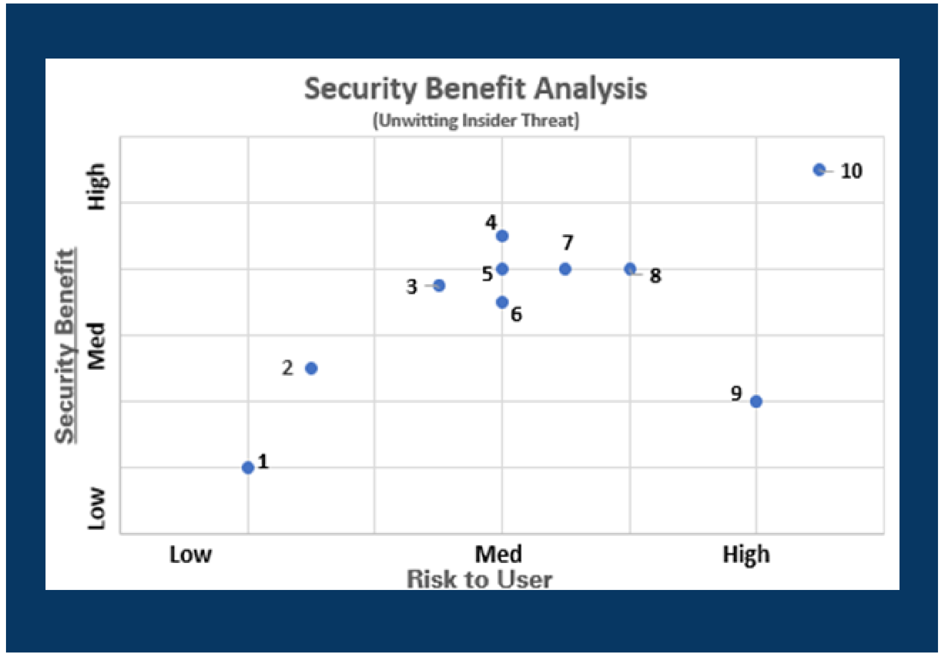
Discarded Mitigations

1. *Require medical device manufacturers to develop SCIF friendly devices*
    - *Only 2% of the population – no business case*
    - *International manufacturing – infeasible*
2. *FDA require medical device security standards*
    - *Likely to occur independent of present discussion*
    - *Medical device design is already HARD*

Bottom Line

Policy guidance looking towards <u>future</u> medical technology

Meeting contradictions of security policy, HR policy, health benefits of IMDs, and truly protecting classified information



Weighing risks/impacts to users and risks to classified information

black hat USA 2020

AUGUST 5-6, 2020
BRIEFINGS

Carrying our Insecurities with Us: the Risks of Implanted Medical Devices in Secure Spaces

Alan J. Michaels, PhD
ajm@vt.edu