Security Update

Security Prioritization Sprint: Background

Police incidents (B 236, Boulder B1)

- Responded with immediate actions (staffing, access controls, etc.)

Planning

- Three External Security Expert Reviews (December 2015)
- Strategic Risk Management Action Plan (MAP) (January 19, 2017)
- ERM Organizational Risk Assessment (February 12, 2017)

Leadership changes

- Acting Director (January 3, 2017)
- Acting Associate for Director Management Resources (February 24, 2017)

What We Are Trying to Protect

- **Our reputation**
- **Our open and collaborative research environment**
  - Our ability to do world-class R&D
  - Foreign Guest Researchers (FGRs) and Foreign National Visitors (FNVs)
- **Our IT systems**
- **Our people**
  - Employees, Associates, Visitors
- **Our facilities and equipment**
  - Our laboratories and office spaces, our user facilities
- **Our information and technology**
  - Sensitive, classified, proprietary, subject to export control regulations

Sprint Charge from Acting NIST Director (Feb. 7, 2017)

Develop an action plan that holistically prioritizes security needs, and mitigating measures, within NIST's numerous activities and mission.

- Provide a rank-ordered list of the security risks/threats, with ranking based on potential impact to the NIST mission.
- Complete within 30 days. Speed is more important than accuracy. Any serious unresolved issues with content should be noted.
- The NIST safety framework (in which risk is based on the potential severity of exposure to a "hazard" and the likelihood of exposure), or equivalent, should be used for assessing risk

Sprint Scope

- Systemic security weaknesses
- Undesirable event risks
- Gaithersburg and Boulder

Sources of Pertinent NIST Security Risk Information

- Three External Security Expert Reviews
- Recent Antiterrorism Risk Assessments (ATRAs) Conducted by the Department of Commerce Office of Security (OSY)
- MR-10 [*Strategic Risk Management Action Plan (MAP): NIST Top Mission Support Risks,* Chapter 10, Security]
- ERM Organizational Risk Assessment
- NIST Manager Interviews

Subject Matter Expertise

- Reports – Three external security experts
- ATRAs – OSY
- MR-10 – NIST and OSY
- ERM organizational risk assessment – NIST and OSY
- Sprint – NIST with assistance from OSY

Systemic Security Weaknesses

Deficiencies in organizational structure, leadership, management, culture, and systems, processes, and services, all as they relate to security

Systemic security weaknesses:

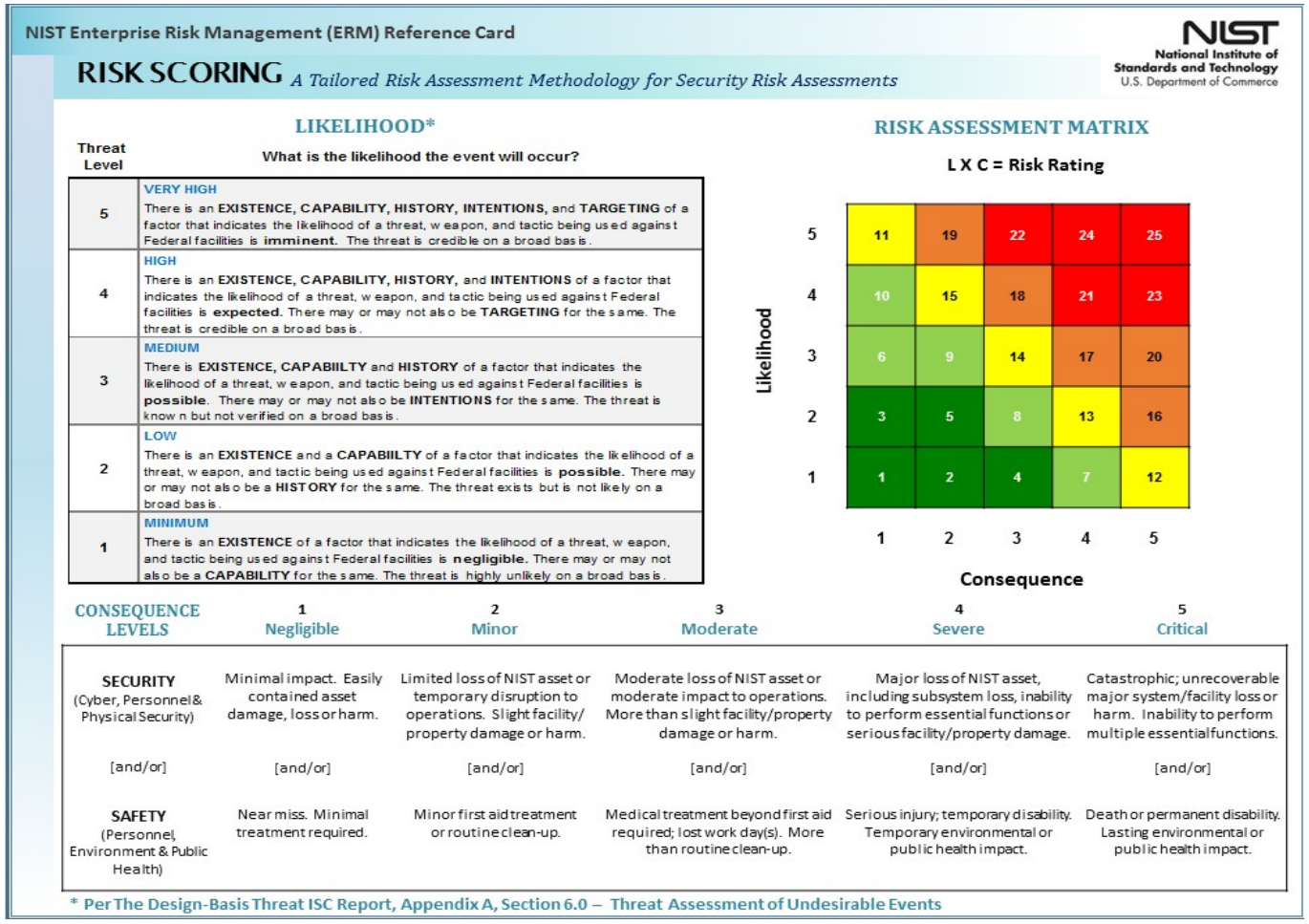
- Less than Optimal Organizational Arrangements
- Lack of Leadership in Establishing a Positive Security Culture
- Significant Gaps in the NIST Security Program

Undesirable Event Risks

- Undesirable event – An incident that has an adverse impact on the facility occupants or visitors, operation of the facility, or mission of the agency.
- Undesirable event risks – The result of systemic security weaknesses, which manifest themselves in vulnerabilities in the control environment that increase the likelihood of undesirable events occurring.

- From the Interagency Security Committee (ISC) Standard
  - 30 undesirable events: active shooter, arson, assault, suicide-homicide bomber, theft, vehicle-borne improvised explosive device, workplace violence, …
- Added by the Report Lead
  - Export Control Violation – Foreign Guest Researcher, Foreign National Visitor

Security Risk Assessment Matrix



NIST Enterprise Risk Management (ERM) Reference Card

NIST National Institute of Standards and Technology U.S. Department of Commerce

RISK SCORING *A Tailored Risk Assessment Methodology for Security Risk Assessments*

LIKELIHOOD*

What is the likelihood the event will occur?

Threat Level	
5	**VERY HIGH** There is an **EXISTENCE, CAPABILITY, HISTORY, INTENTIONS,** and **TARGETING** of a factor that indicates the likelihood of a threat, weapon, and tactic being used against Federal facilities is **imminent.** The threat is credible on a broad basis.
4	**HIGH** There is an **EXISTENCE, CAPABILITY, HISTORY,** and **INTENTIONS** of a factor that indicates the likelihood of a threat, weapon, and tactic being used against Federal facilities is **expected.** There may or may not also be **TARGETING** for the same. The threat is credible on a broad basis.
3	**MEDIUM** There is **EXISTENCE, CAPABIILTY** and **HISTORY** of a factor that indicates the likelihood of a threat, weapon, and tactic being used against Federal facilities is **possible.** There may or may not also be **INTENTIONS** for the same. The threat is known but not verified on a broad basis.
2	**LOW** There is an **EXISTENCE** and a **CAPABIILTY** of a factor that indicates the likelihood of a threat, weapon, and tactic being used against Federal facilities is **possible.** There may or may not also be a **HISTORY** for the same. The threat exists but is not likely on a broad basis.
1	**MINIMUM** There is an **EXISTENCE** of a factor that indicates the likelihood of a threat, weapon, and tactic being used against Federal facilities is **negligible.** There may or may not also be a **CAPABILITY** for the same. The threat is highly unlikely on a broad basis.

RISK ASSESSMENT MATRIX

L X C = Risk Rating

Likelihood \ Consequence	1	2	3	4	5
5	11	19	22	24	25
4	10	15	18	21	23
3	6	9	14	17	20
2	3	5	8	13	16
1	1	2	4	7	12

CONSEQUENCE LEVELS	1 Negligible	2 Minor	3 Moderate	4 Severe	5 Critical
SECURITY (Cyber, Personnel & Physical Security)	Minimal impact. Easily contained asset damage, loss or harm.	Limited loss of NIST asset or temporary disruption to operations. Slight facility/ property damage or harm.	Moderate loss of NIST asset or moderate impact to operations. More than slight facility/property damage or harm.	Major loss of NIST asset, including subsystem loss, inability to perform essential functions or serious facility/property damage.	Catastrophic; unrecoverable major system/facility loss or harm. Inability to perform multiple essential functions.
[and/or]	[and/or]	[and/or]	[and/or]	[and/or]	[and/or]
SAFETY (Personnel, Environment & Public Health)	Near miss. Minimal treatment required.	Minor first aid treatment or routine clean-up.	Medical treatment beyond first aid required; lost work day(s). More than routine clean-up.	Serious injury; temporary disability. Temporary environmental or public health impact.	Death or permanent disability. Lasting environmental or public health impact.

* Per The Design-Basis Threat ISC Report, Appendix A, Section 6.0 – Threat Assessment of Undesirable Events

Risk = Threat Level x Vulnerability x Consequence

ISC Standard Security Criteria

- Security of Critical Areas
- CCTV Coverage
- CCTV Monitoring and Recording
- Intrusion Detection System Coverage
- Guard Fixed-Post Exterior
- Guard Patrols
- Occupant Emergency Plan
- Security Awareness Training
- Pedestrian Access to Site
- Site Lighting
- Vehicle Screening
- Protection of Air Intakes
- Employee Access Control
- Visitor Access Control
- After-Hours Access Control
- Perimeter Doors and Door Locks

Sprint Report Results

- **Holistic prioritized list of 45 security vulnerabilities and mitigations**

Charge February 7, 2017; report March 22, 2017

Subsequent Developments

Date	Action
Apr 17, 2017	Sprint report presented by Report Lead to NIST Security Advisory Board (SAB)
Apr 27, 2017	SAB concurrence on initial set of 12 prioritized actions
May 2, 2017	Prioritized actions submitted by SAB Chair to Acting NIST Director
May 4, 2017	Prioritized actions accepted by Acting NIST Director
May 9, 2017	Charge from Acting NIST Director to SAB Chair to develop action plans
May 10, 2017	Charge from SAB Chair to Report Lead to lead the development of action plans
In progress	Development of action plans

Twelve Prioritized Actions

The 12 prioritized actions together address the top 25 security vulnerabilities

1. **Identify the optimal organizational fit for security**
2. **Establish clear baseline security requirements and roles, responsibilities, authorities, and accountabilities (R2A2S) for the NIST staff**
3. **Exercise leadership and improve accountability and understanding**
4. **Create advisory group like the NIST Executive Safety Committee to engage NIST leadership in the establishment of the NIST security program**

Twelve Prioritized Actions

5. **Establish and implement security standards for NIST spaces warranting enhanced security**

6. **Establish clear NIST security program requirements and R2A2s beyond the baseline**

7. **Expand security awareness training (on topics such as active shooter, workplace violence, general crime prevention measures, suspicious packages)**

9. **Take actions to protect against export control violations involving Foreign Guest Researchers and Foreign National Visitors**

NOTE: Have omitted 4 of the 12 prioritized actions

Security Sprint

Questions?