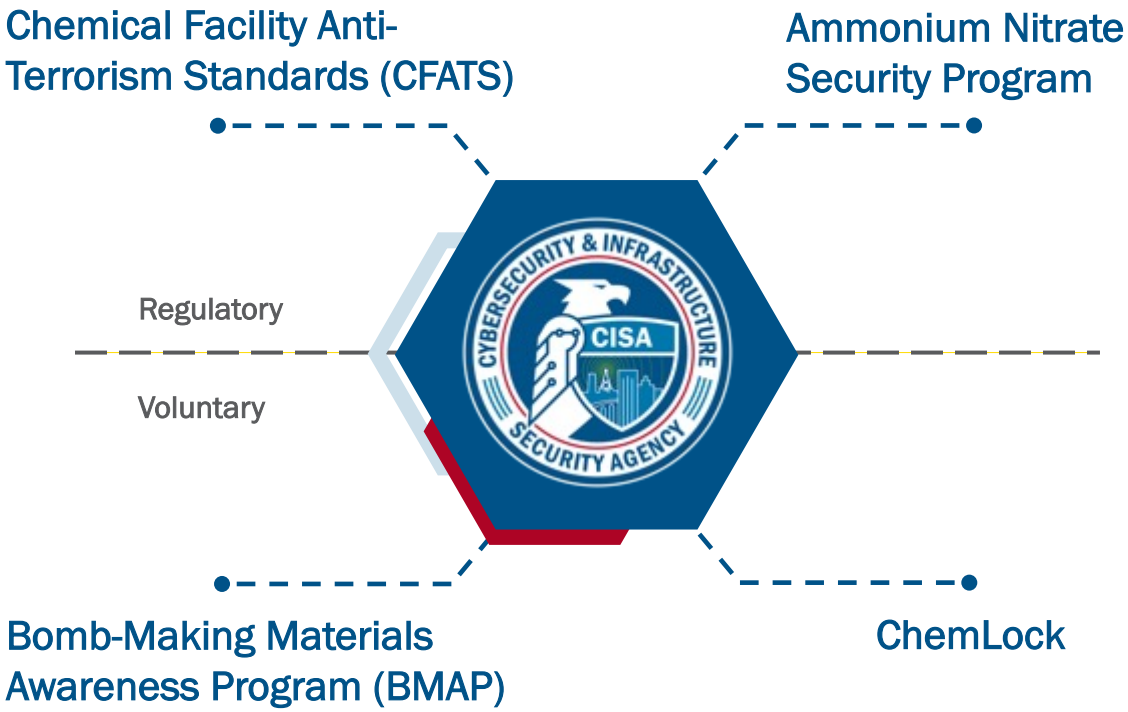
AN INSIDE JOB:
PROTECTING CHEMICAL FACILITIES FROM INSIDER EXPLOITATION

Critical Infrastructure Protection and Resilience North America (CIPRNA)
April 7, 2022

Todd Klessman
April 7, 2022

CISA Chemical Security Overview



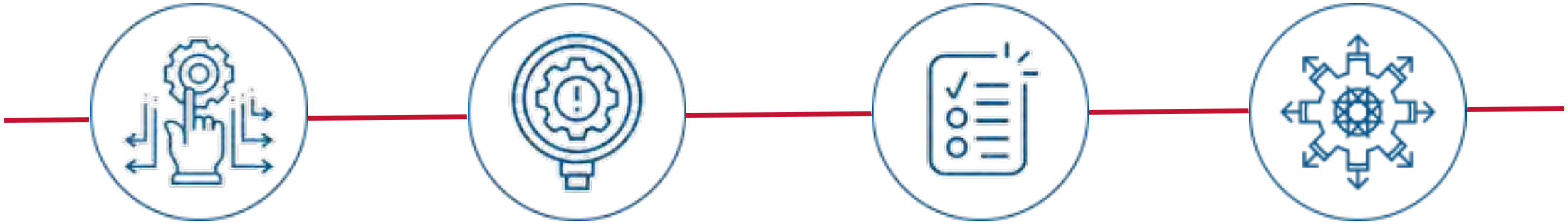
CFATS identifies facilities with chemicals that are high-risk and works with them to develop tailored security plans that meet risk-based standards.

CFATS 18 Risk-Based Performance Standards

1) Restrict Area Perimeter
2) Secure Site Assets
3) Screen and Control Access
4) Deter, Detect, Delay
5) Shipping, Receipt, and Storage
6) Theft and Diversion
7) Sabotage
8) Cyber
9) Response
10) Monitoring
11) Training
12) Personnel Surety
13) Elevated Threats
14) Specific Threats, Vulnerabilities, or Risks
15) Reporting Significant Security Incidents
16) Significant Security Incidents and Suspicious Activities
17) Officials and Organization
18) Records

Personnel Surety Background Checks
Verify and Validate Identity
Check Criminal History
Validate Legal Authorization to Work in the U.S.
Identify People with Terrorist Ties

Key Steps to Insider Threat Mitigation



Define

Detect and Identify

Assess

Manage

cisa.gov/insider-threat-mitigation

Definition of Insider Threat

An Insider Threat is the **potential for an insider to use their authorized access or special understanding** of an organization to harm that organization.

Harm can include **malicious, complacent, or unintentional acts** that negatively affect the organization, its data, personnel, facilities, or associated resources.

Types of Insider Threat

Unintentional

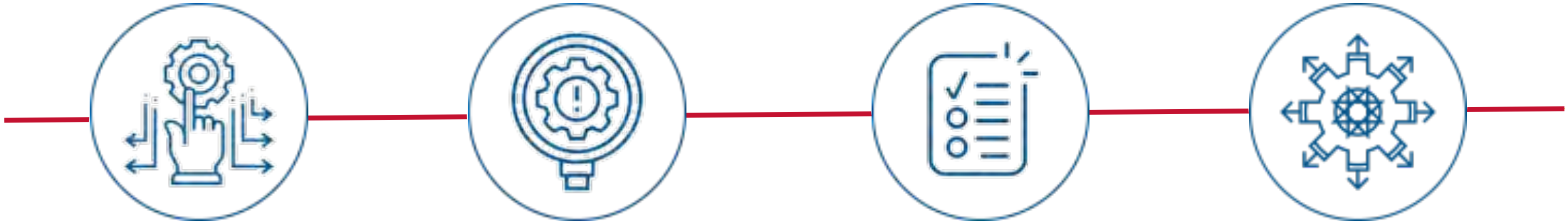
Negligent: Insiders expose an organization to a threat by their carelessness.

Accidental: Human error results in a mistake that causes unintended risk to an organization.

Intentional/Malicious

Insiders intentionally take actions that harm an organization for personal benefit or grievance.

Key Steps to Insider Threat Mitigation



Define

Detect and Identify

Assess

Manage

cisa.gov/insider-threat-mitigation

Identifying the Threat

No standard profile – impacted by:

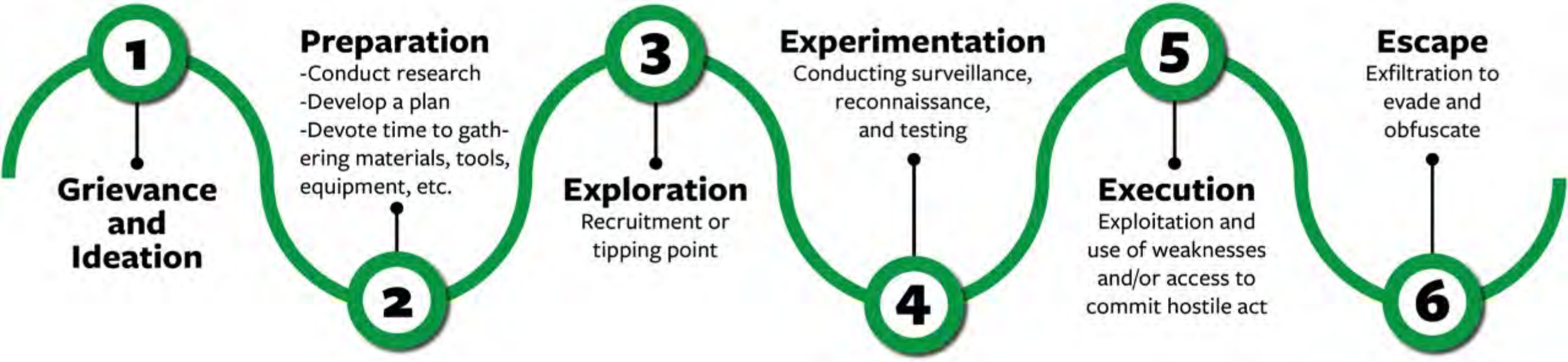
Personal Predispositions - Contextual Stressors - Patterns of Suspicious Behaviors and Actions

Seldom act impulsively

Moving from Idea to Action

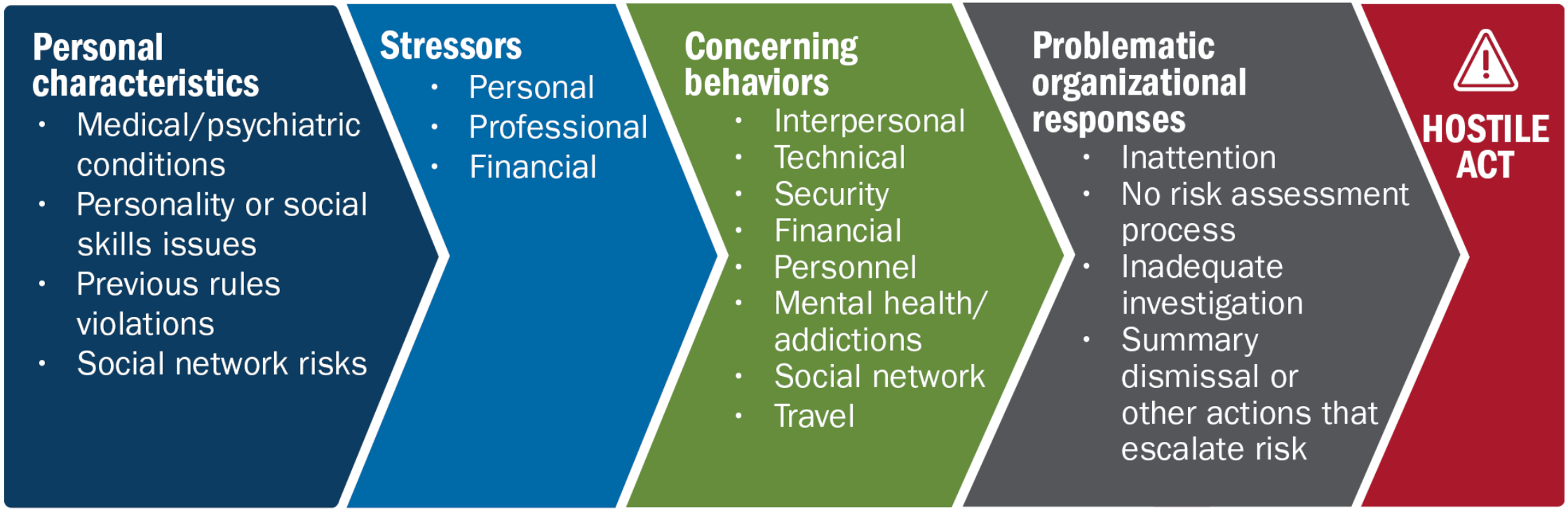
Red flags involve changes in baseline behavior

Usually exhibit observable patterns



Factors Along the Path to Insider Risk

Importance of the "whole person" concept



Identification is Possible!

In **42 computer system sabotage incidents** throughout the critical infrastructure sectors:

of perpetrators communicated negative feelings, grievances, and/or an interest in causing harm

- **92%** verbally
- **12%** via email

of the time, others had information about the insiders' plans, intentions, and/or activities

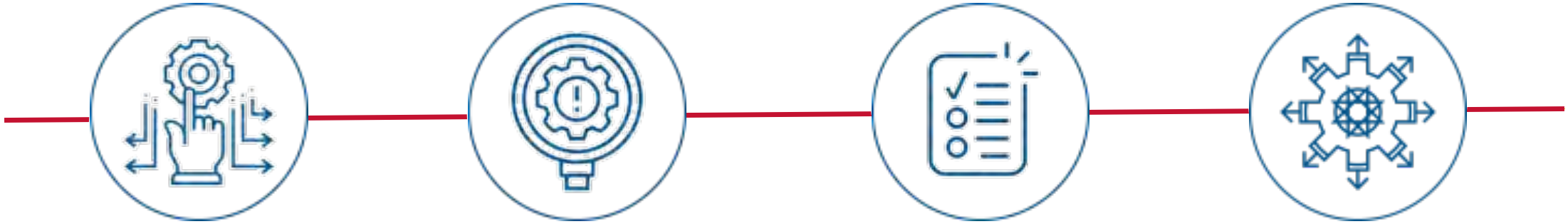
- **64%** coworkers
- **21%** friends
- **14%** family members
- **14%** someone involved with the incident

In **27 violent attacks in public spaces**:

of the attackers made concerning comments

- Expressing **interest in previous attackers**
- Making or suggesting **racist and misogynistic comments**
- Referencing a **desire to purchase a gun**
- Expressing **aspirations to commit future violence**

Key Steps to Insider Threat Mitigation



Define

Detect and Identify

Assess

Manage

cisa.gov/insider-threat-mitigation

Insider Threat Program Development

Build upon existing policies, physical security procedures, IT, and cybersecurity programs

Borrow available best practices, concepts, and tools from available sources:

Examples:

National Insider Threat Task Force

Insider Threat Mitigation Guide

Insider Risk Mitigation Program Evaluation (IRMPE)

Include these four mission areas:

- Plan
- Organize & Equip
- Train & Execute
- Evaluate & Improve

Preventing the Next Insider Threat

1

Train employees to recognize behaviors that indicate a progression

2

Instill a positive culture for reporting

3

Establish Threat Management Team and develop intervention capabilities

Awareness + Action = Prevention

Conclusion

There is no "one-size-fits-all" approach to threat management.
Having an effective Insider Threat Mitigation Program can protect against an insider incident having wide-ranging consequences with devastating outcomes and long-term, negative impacts.

Principles and Keys for Success

- **Promote a protective and supportive culture** throughout the organization.
- **Safeguard organizational valuables** while protecting privacy, rights, and liberties.
- **Remain adaptive** as the organization evolves and its risk tolerance changes.
- **Focus on prevention** and helping people versus just catching them doing things wrong.
- **Employ a balance of positive and negative incentives**, promoting employee satisfaction and performance while avoiding overly aggressive reactions following notification of a threat.

Chemical Security:

cisa.gov/chemical-security

CFATS@hq.dhs.gov

ChemLock@cisa.dhs.gov

Insider Threat:

cisa.gov/insider-threat-mitigation

InTmitigation@cisa.dhs.gov


CYBERSECURITY & INFRASTRUCTURE
SECURITY AGENCY
CISA