The reporting and investigative templates are not intended to provide any organization with the authority to perform activities that they are otherwise not able to perform under applicable law, regulation, and policy. Consult with your legal counsel before implementing these forms in your organization.

INCIDENT DETAILS

1	**Incident Description**	*Outline incident in further detail (i.e. witness statement, etc.). What IT systems were compromised? What technology identified the breach (if applicable)?"*

2	**Concern Type**	*Examples include: Verbal/Written Threats; Terrorism/Violent Extremism; Personal Conduct; Financial Considerations; Substance Abuse; Behavioral Considerations; Criminal Conduct; Mishandling Protected Information; Misuse of Information Technology; Espionage; Financial/Intellectual Property Theft; Other*

3	**Has the appropriate security professional been notified?**	*Yes*	*No*	*N/A*
4	**Has the Insider Threat Management Team been notified?**	*Yes*	*No*	*N/A*

INFORMATION ON THE PERSON OF INTEREST

5	Name
6	Job Title
7	Labor Category
8	Clearance Level / Special Access
9	Network Privileges
10	Equipment Used in Incident
11	Office Location
12	Incident Date or Date Range
13	Incident Time(s)

INVESTIGATOR/INTAKE OFFICIAL'S INFORMATION

14	Name
15	Contact Information
16	Position

ADDITIONAL INFORMATION

| 17 | **Initial Recommendations** | *Does law enforcement need to be involved? What action needs to occur to keep individuals safe?* |

| 18 | **How was the suspicious activity detected?** | *What activity occurred? What was the individual's main motivation (if known)? Were any organizational policies violated? How were the security policies/procedures evaded if possible? What action did the organization take to mitigate and prevent an incident?* |

| 19 | **Next Steps, Follow-up, and Conclusion** | *What actions did the organization take? Were consequences for the individual recommended to HR such as a formal warning, suggested counseling, or termination? Was the matter sent to law enforcement for further investigation? Were witness interviews conducted? What action must come next in this particular instance?* |

| 20 | **Recommendations / Updates / Changes to Make** | *What security considerations should the organization address? What changes need to be made to protect the organization's high-value assets? Did the reporting pathway lead to a successful mitigation or prevention? If not, what security gap needs to be addressed? Is increased monitoring of the individual needed?* |

REPORT REVIEWED BY

Name   Title

Law Enforcement Investigation Number (if   Investigating Office (if applicable)   Date
applicable)