# Government Problem Statement

| | | |
|---|---|---|
| **16.** | **Problem Statement Title** | Use AI to assist in post-incident forensic analysis by identifying the attack vector, compromised assets, and timeline of a cybersecurity breach. |
| | **Description** | Using AI to assist in post-incident forensic analysis involves leveraging advanced machine learning algorithms and data analytics to quickly and accurately identify the attack vector, compromised assets, and the timeline of a cybersecurity breach. Traditional forensic analysis often relies on manual methods, which can be time-consuming and error-prone. AI-enhanced tools can automate and streamline this process, enabling faster and more thorough investigations.<br><br>Once a cybersecurity breach occurs, AI systems can analyze large volumes of data from various sources such as network logs, endpoint activity, server communications, and security alerts. By correlating and analyzing this data in real-time, AI can identify the attack vector, which is the method through which the attacker infiltrated the system, whether through phishing, malware, vulnerabilities, or other tactics. |
| | **Department** | Department IT & Electronics |
| | **Sector** | Cybersecurity & Cyber Threats |