**The Necessity of an Internal DFIR Team**

Kevin D. Winfield

Cybersecurity Management, Murray State University

CYS 640: Incident Management and Business Continuity

Dr. Randall Joyce

March 4, 2025

**Tantalum Defense Technologies**  
**Senior Executive Report: The Necessity of an Internal DFIR Team**  
**Prepared By: CISO**  
**Date: 2025-03-04**

**Executive Summary**

Tantalum Defense Technologies provides cloud services for tactical networks to the Department of Defense (DoD). Given the ever-growing cybersecurity threats, the company is at risk of sophisticated cyberattacks that could disrupt operations, compromise sensitive data, and weaken national security. This report evaluates the need for an internal Digital Forensics and Incident Response (DFIR) team, detailing potential threats, business impacts, and cost considerations. A DFIR team will provide rapid response capabilities, minimize disruptions, and ensure compliance with DoD cybersecurity regulations. A cybersecurity breach or malware attack could lead to significant financial losses, regulatory penalties, and reputational damage. The DFIR team will be responsible for identifying, containing, mitigating, and recovering from security incidents efficiently. This report also examines past industry breaches to highlight the importance of proactive security measures. Additionally, it provides an in-depth business impact analysis, assesses potential costs, and outlines necessary regulatory compliance standards.

**Current Threat Landscape**

The defense industry is a prime target for nation-state actors, cybercriminals, and insider threats. Attack vectors include ransomware, supply chain attacks, insider threats, and advanced persistent threats (APTs). With increased reliance on cloud-based infrastructure, vulnerabilities in cloud services present a major concern.

**Key Threats in the Defense Sector**

Ransomware Attacks:

If Tantalum Defense Technologies falls victim to a ransomware attack, adversaries could encrypt critical cloud-based tactical network services, making them inaccessible to DoD operations. The exposure of classified DoD communications due to double-extortion tactics would severely damage the company’s reputation and may result in contract termination. Incident response costs could exceed millions, impacting financial stability.

Supply Chain Compromise:

As a cloud service provider, Tantalum Defense Technologies integrates multiple third-party vendors. A supply chain compromise at any level could serve as an entry point for adversaries to access DoD networks. A compromised vendor update could result in backdoors within mission-critical cloud systems, allowing unauthorized data exfiltration. Such an event would result in a loss of trust from the DoD, requiring extensive remediation efforts and compliance audits.

Insider Threats:

Malicious insiders or negligent employees at Tantalum Defense Technologies could expose sensitive data related to DoD operations. A disgruntled employee with privileged access could intentionally sabotage cloud infrastructure, leading to downtime in tactical network communications. To mitigate this risk, implementing behavioral analytics and strict access control policies is essential.

Advanced Persistent Threats (APTs):

Nation-state-backed APT groups may target Tantalum Defense Technologies to gain long-term, persistent access to DoD cloud services. If an APT gain a foothold in the infrastructure, it could conduct prolonged espionage, siphoning critical DoD intelligence.

APTs often go undetected for months, making rapid forensic analysis and incident response crucial to limiting damage.

Zero-Day Exploits:

Tantalum Defense Technologies operates cloud environments that may contain undiscovered vulnerabilities. If adversaries exploit a zero-day vulnerability, they could compromise the entire cloud infrastructure. A zero-day exploit could lead to the deployment of rootkits or malware that persist within cloud systems, making remediation challenging. Proactive threat hunting and collaboration with security researchers are necessary to minimize risks.

Cloud Infrastructure Vulnerabilities:

If Tantalum Defense Technologies' cloud systems are misconfigured, adversaries may gain unauthorized access to classified DoD data. Poorly implemented identity and access management (IAM) policies could allow attackers to escalate privileges and control mission-critical environments. Secure access service edge (SASE) solutions and Zero Trust security frameworks should be prioritized to mitigate these risks.

Distributed Denial-of-Service (DDoS) Attacks:

A well-orchestrated DDoS attack against Tantalum Defense Technologies could cripple cloud-based DoD communication systems. Given the real-time nature of tactical networks, a DDoS-induced service outage would severely impact military operations. Cloud-based DDoS mitigation services must be implemented to ensure service availability under attack conditions. Employees at Tantalum Defense Technologies may fall victim to spear-phishing campaigns designed to steal credentials. Attackers impersonating DoD officials could manipulate employees into divulging sensitive cloud system access credentials. Mandatory security awareness training and phishing simulations are essential to reducing human error vulnerabilities.

**Notable Breaches in the Defense Industry**

SolarWinds Breach

The SolarWinds cyberattack was one of the most sophisticated and damaging supply chain attacks in history. Attackers, believed to be affiliated with a nation-state, inserted malicious code into updates of the widely used SolarWinds Orion software. This malicious update was distributed to thousands of organizations, including government agencies and defense contractors, providing attackers with unauthorized access to sensitive networks. Once inside, the threat actors remained undetected for months, exfiltrating critical data and establishing persistent access.

The attack had far-reaching consequences, affecting not only private companies but also critical U.S. government agencies, including the Department of Defense and Department of Homeland Security. The breach highlighted vulnerabilities in the software supply chain, demonstrating how a single compromised vendor could be leveraged to infiltrate multiple high-value targets. For Tantalum Defense Technologies, a similar attack on one of its third-party providers could have catastrophic consequences, leading to unauthorized access to DoD cloud environments, data exfiltration, and service disruptions. Implementing stronger vendor risk management and threat intelligence sharing would be critical in mitigating such risks.

Lockheed Martin Cyber Attack (2011)

In 2011, Lockheed Martin, one of the largest defense contractors in the world, was targeted in a cyberattack involving the compromise of RSA SecurID tokens. Attackers first breached RSA, the security company responsible for providing authentication systems to defense firms and stole confidential encryption keys associated with SecurID tokens. Using this information, they launched a targeted attack against Lockheed Martin’s network, attempting to bypass multi-factor authentication (MFA) mechanisms.

Although Lockheed Martin detected and mitigated the attack before significant data loss occurred, the breach underscored the vulnerabilities in widely used authentication systems. The attack prompted major changes in how defense contractors approached identity and access management, leading to increased adoption of stronger cryptographic authentication methods. For Tantalum Defense Technologies, an attack of this nature could compromise cloud-based authentication systems, allowing unauthorized users to access classified DoD resources. Strengthening identity security, implementing hardware security modules (HSMs), and enforcing continuous authentication are necessary steps to prevent similar incidents.

Boeing Ransomware Attack (2018)

In 2018, a ransomware attack briefly halted Boeing's manufacturing operation. The attack was attributed to the WannaCry ransomware variant, which exploited a known vulnerability in Microsoft Windows operating systems. While the attack did not cause significant operational damage, it highlighted the persistent risks posed by ransomware, particularly in critical industries such as aerospace and defense.

Ransomware attacks have evolved in sophistication since the Boeing incident, with modern variants incorporating double extortion tactics—where attackers not only encrypt data but also threaten to leak sensitive information. If Tantalum Defense Technologies were targeted by ransomware, it could lead to downtime in cloud-based DoD communications systems, the exposure of classified data, and potential regulatory penalties. The company must implement proactive measures such as network segmentation, continuous backups, and endpoint detection and response (EDR) solutions to prevent and mitigate ransomware threats.

These case studies illustrate the potential consequences of cybersecurity incidents for Tantalum Defense Technologies. Each breach provides valuable lessons on the importance of vendor security, authentication integrity, and ransomware resilience. By learning from past incidents and strengthening internal security capabilities, Tantalum Defense Technologies can better protect its DoD cloud services and maintain operational readiness in the face of evolving cyber threats.

**Security Breach Scenario**

In this scenario, an advanced persistent threat (APT) group, likely backed by a nation-state, targets Tantalum Defense Technologies due to its role as a cloud service provider for the DoD. The attack begins with a sophisticated spear-phishing campaign aimed at senior executives and IT administrators, tricking them into downloading a malicious attachment. Once inside the network, the attackers use stolen credentials to move laterally, gaining unauthorized access to critical cloud systems.

After several weeks of covert activity, the threat actors successfully extracted classified data from the Department of Defense, encompassing operational plans and secure communication protocols. Simultaneously, they deploy ransomware across the organization’s cloud infrastructure, encrypting mission-critical data and disrupting key services, including tactical network communications. The attack is discovered only when DoD clients report service disruptions and classified information begins appearing on dark web forums.

**Effects and Damages of the Breach:**

1.Operational Disruption:

Tactical network communications for deployed military units are impacted, leading to delays in real-time intelligence sharing and mission execution. Critical DoD applications hosted on Tantalum Defense Technologies’ cloud platform experience outages, requiring emergency restoration efforts.

2.Financial Losses:

Incident response and forensic investigations cost the company millions of dollars in immediate remediation expenses. Ransom demands from attackers, if considered, could add financial burden and ethical dilemmas regarding compliance with DoD cybersecurity policies. Loss of contracts and business opportunities due to loss of confidence from the DoD and other defense contractors.

3.Data Compromise:

Unauthorized access to classified DoD data leads to national security concerns, potentially exposing military strategies and technological advancements. Intellectual property theft impacts proprietary cloud-based defense solutions, reducing Tantalum Defense Technologies’ competitive edge.

4.Regulatory and Legal Repercussions:

Failure to secure sensitive DoD data results in non-compliance with DFARS, CMMC, and FISMA regulations, leading to federal investigations and fines. Potential lawsuits from DoD and defense partners for breach of contractual obligations regarding data protection and cybersecurity standards.

5.Reputational Damage:

Loss of trust from DoD clients, leading to reduced future contract opportunities. Negative media coverage and scrutiny from government agencies and industry regulators.

6.Extended Recovery Timeline:

Full system restoration, security patching, and regulatory audits could take months, significantly affecting business continuity. Mandatory cybersecurity enhancements and staff retraining efforts would require additional investments in security infrastructure and personnel.

**Business Impact Analysis (BIA)**

The Business Impact Analysis (BIA) evaluates the potential consequences of a cybersecurity incident, helping Tantalum Defense Technologies prioritize critical systems, set recovery objectives, and allocate resources effectively. Given the company’s role as a cloud service provider for DoD operations, disruptions could have significant national security implications.

**Critical Cloud Services Supporting the DoD**

Tantalum Defense Technologies offers a range of cloud-based services that are crucial for Department of Defense operations. Any compromise or disruption to these services could severely impact national security, military communications, and tactical readiness. The following cloud services are identified as critical:

1.Secure Communications Platform

* Ensures real-time, encrypted communication between deployed military units, intelligence teams, and command centers.
* Any service disruption would delay battlefield coordination, increasing risks for military personnel.

2.Encrypted Data Storage and Processing

* Manages and secures classified DoD data, including operational intelligence, mission reports, and supply chain logistics.
* A breach or loss of integrity could expose sensitive data to adversaries, compromising national security.

3.AI-Driven Battlefield Analytics

* Provides real-time data processing and threat assessment using machine learning and artificial intelligence.
* Service interruptions would hinder DoD’s ability to process real-time intelligence, impacting strategic decision-making.

4.Zero-Trust Authentication and Identity Management

* Supports identity verification and access controls for DoD personnel using cloud infrastructure.
* A compromise in authentication services could lead to unauthorized access, increasing insider threat risks.

5.Tactical Network Orchestration

* Manages and optimizes battlefield network deployments, ensuring seamless connectivity in combat zones.
* Disruptions could lead to loss of connectivity, affecting command-and-control operations.

**Impact of Disruptions on Cloud Services**

|  |  |  |
| --- | --- | --- |
| **Cloud Service** | **Impact Level** | **Estimated Downtime Cost (per day)** |
| Secure Communications | High | $3 million |
| Encrypted Data Storage | Critical | $7 million |
| AI-Driven Battlefield Analytics | Medium | $2 million |
| Zero-Trust Authentication | High | $4 million |
| Tactical Network Orchestration | Critical | $5 million |

**Recovery Objectives**

* **Recovery Time Objective (RTO):**
  + Secure Communications: 2 hours
  + Encrypted Data Storage: 4 hours
  + AI-Driven Battlefield Analytics: 8 hours
  + Zero-Trust Authentication: 2 hours
  + Tactical Network Orchestration: 4 hours
* **Recovery Point Objective (RPO):**
  + Secure Communications: Near-zero data loss
  + Encrypted Data Storage: Near-zero data loss
  + AI-Driven Battlefield Analytics: 15 minutes
  + Zero-Trust Authentication: Near-zero data loss
  + Tactical Network Orchestration: 30 minutes

**Importance of an Internal DFIR Team**

Tantalum Defense Technologies operates in a high-risk environment where rapid and effective response is critical. A dedicated internal Digital Forensics and Incident Response (DFIR) team ensures that the company can quickly detect, analyze, contain, and remediate security incidents without relying solely on external third-party providers. Below are the key reasons why having an internal DFIR team is essential:

1. Faster Incident Response and Mitigation

* An internal DFIR team reduces the time needed to detect and contain security threats, minimizing the potential impact of a cyberattack.
* Immediate response to threats ensures that tactical cloud-based DoD operations remain secure and operational.
* Internal expertise allows for real-time incident triage and forensic analysis without external delays.

2. Enhanced Data Security and Confidentiality

* As a defense contractor, Tantalum Defense Technologies handles sensitive DoD data that should not be exposed to third-party DFIR providers.
* Keeping incident response in-house ensures tighter control over classified information, reducing exposure to potential insider threats.

3. Regulatory and Compliance Alignment

* The DoD enforces strict cybersecurity regulations, including DFARS, CMMC, and FISMA, which require stringent incident response measures.
* An internal DFIR team ensures compliance with federal cybersecurity mandates, reducing the risk of penalties or contract revocations.

4. Proactive Threat Hunting and Risk Management

* DFIR teams not only respond to incidents but also proactively hunt for threats within Tantalum Defense Technologies’ network.
* They can identify vulnerabilities before attackers exploit them, reducing the risk of zero-day attacks and persistent threats.

5. Cost Savings and Long-Term ROI

* While developing an internal DFIR team requires upfront investment, it significantly reduces long-term costs associated with third-party response teams, incident-related downtime, and regulatory fines.
* Having a dedicated team enables faster resolution, reducing financial losses from prolonged service disruptions.

Benefits of an internal DFIR Team

|  |  |
| --- | --- |
| **Benefit** | **Description** |
| Faster Response Time | Immediate detection and containment of threats. |
| Confidentiality | Protects sensitive DoD data from exposure. |
| Cost Efficiency | Reduces reliance on expensive external forensic services. |
| Compliance Assurance | Ensures adherence to DoD regulations. |
| Proactive Defense | Enables continuous threat hunting and network monitoring to prevent breaches. |

**DFIR Approach/Processes**

The Digital Forensics and Incident Response (DFIR) team at Tantalum Defense Technologies will follow a structured approach aligned with DoD cybersecurity regulations and industry best practices. The primary objective is to rapidly detect, contain, and recover from cyber incidents while maintaining compliance with frameworks such as NIST 800-171, CMMC, DFARS, and FISMA.

1. Incident Detection and Identification

* Utilize Security Information and Event Management (SIEM) solutions to monitor network activity and detect anomalies.
* Implement Endpoint Detection and Response (EDR) and Threat Intelligence Platforms for proactive threat hunting.
* Establish Automated Incident Detection Mechanisms based on MITRE ATT&CK tactics and techniques.
* Conduct continuous log analysis and correlation to identify indicators of compromise (IOCs) in real-time.

2. Incident Containment

* Activate network segmentation to isolate affected systems and prevent further lateral movement.
* Enforce role-based access control (RBAC) and Zero Trust principles to limit unauthorized access.
* Deploy containment strategies based on attack type, including sandboxing malware samples for analysis.
* Work in alignment with DoD’s Cyber Incident Handling Program (CJCSM 6510.01B) to coordinate containment strategies.

3. Eradication and Remediation

* Conduct digital forensic analysis to determine root cause and scope of the attack.
* Remove malicious code, patch vulnerabilities, and restore affected systems using secure baseline configurations.
* Implement automated remediation scripts to prevent reinfection and strengthen system defenses.
* Coordinate with DoD Cyber Crime Center (DC3) for forensic analysis and evidence handling.

4. Recovery and System Restoration

* Restore compromised systems from secure backups to prevent data loss.
* Validate integrity of restored systems through hash verification and security scans.
* Conduct post-recovery testing to confirm that security patches and mitigations are effective.
* Reintegrate affected systems into the network following DoD Risk Management Framework (RMF) procedures.

5. Post-Incident Analysis and Reporting

* Conduct a detailed post-mortem analysis to evaluate response effectiveness and identify areas for improvement.
* Generate and submit an Incident Report to the DoD in compliance with DFARS 252.204-7012 requirements.
* Update Incident Response Playbooks to incorporate lessons learned and improve future readiness.
* Conduct staff training and awareness programs based on new attack trends and vulnerabilities.

6. Continuous Monitoring and Threat Intelligence Integration

* Engage in threat intelligence sharing with CISA, DC3, and National Defense ISAC to stay ahead of evolving cyber threats.
* Conduct regular red team vs. blue team exercises to test incident response effectiveness.
* Leverage machine learning-based anomaly detection to enhance proactive threat identification.
* Continuously update defense mechanisms to align with evolving DoD cybersecurity directives.

**Developing an Internal DFIR Team**

The costs associated with developing and maintaining an internal DFIR team include staffing, tools, training, and ongoing operational expenses.

Staffing Costs

|  |  |
| --- | --- |
| **Role** | **Estimated Salary (Annual)** |
| Incident Response Manager | $180,000 |
| Forensic Analyst | $140,000 |
| Threat Intelligence Analyst | $130,000 |
| Security Operations Center (SOC) Analyst | $120,000 |
| System Security Engineer | $135,000 |
| Compliance Officer | $125,000 |
| Total Annual Staffing Costs | $830,000 |

Tools and Technology Investments

|  |  |
| --- | --- |
| **Tool/Technology** | **Estimated Cost (Annual)** |
| Security Information and Event Management (SIEM) | $250,000 |
| Endpoint Detection and Response (EDR) | $200,000 |
| Network Traffic Analysis (NTA) | $150,000 |
| Threat Intelligence Platform | $100,000 |
| Secure Forensic Workstations | $75,000 |
| Total Tool Investment | $775,000 |

Training and Continuous Education

|  |  |
| --- | --- |
| Training Program | Cost per Year |
| Incident Response & Forensics Training | $50,000 |
| Threat Intelligence Certification Programs | $40,000 |
| Red/Blue Team Cybersecurity Exercises | $30,000 |
| Total Training Cost | $120,000 |

Operational and Maintenance Costs

* Annual maintenance and upgrades for DFIR tools: $200,000
* External compliance audits and assessments: $100,000
* Total estimated O&M: $300,000

Total Estimated Costs for DFIR Team

|  |  |
| --- | --- |
| **Category** | **Cost** |
| Staffing | $830,000 |
| Tools & Technology | $775,000 |
| Training & Education | $120,000 |
| Operations & Maintenance | $300,000 |
| Total Annual Cost | $2,025,000 |

Building an internal DFIR team at Tantalum Defense Technologies is a strategic investment that enhances security resilience, ensures compliance with DoD cybersecurity mandates, and reduces reliance on third-party response teams. While the initial and ongoing costs of maintaining the team amount to approximately $2 million per year, the benefits—including faster incident response, data confidentiality, cost savings, and proactive defense—far outweigh the financial investment. By establishing a well-equipped DFIR team, Tantalum Defense Technologies can safeguard its cloud services, protect national security interests, and maintain operational continuity in the face of evolving cyber threats.

**DoD Regulations and Compliance Requirements**

Tantalum Defense Technologies must adhere to stringent cybersecurity regulations to maintain its position as a DoD cloud services provider. Compliance is critical to ensuring the confidentiality, integrity, and availability of DoD data and systems. Below are the key regulations and frameworks that govern cybersecurity practices within the defense industry.

1. Defense Federal Acquisition Regulation Supplement (DFARS) and NIST 800-171

* DFARS mandates cybersecurity requirements for defense contractors managing Controlled Unclassified Information (CUI).
* Requires compliance with NIST Special Publication 800-171, which outlines 110 security controls related to access control, incident response, risk management, and encryption.
* Failure to comply can result in loss of DoD contracts and fines.

2. Cybersecurity Maturity Model Certification (CMMC)

* Introduced to standardize cybersecurity practices across the defense supply chain.
* Includes five maturity levels ranging from basic cyber hygiene (Level 1) to advanced/progressive cybersecurity practices (Level 5).
* Requires third-party audits to verify compliance, ensuring that contractors properly safeguard sensitive information.
* Tantalum Defense Technologies must achieve at least CMMC Level 3 to manage Controlled Unclassified Information (CUI) for DoD operations.

3. Federal Information Security Modernization Act (FISMA)

* Establish cybersecurity guidelines for federal agencies and contractors.
* Require risk assessments, continuous monitoring, and the implementation of security policies.
* Enforce compliance through audits conducted by the Office of Management and Budget (OMB) and National Institute of Standards and Technology (NIST).

Failure to adhere to DoD regulations:

* Loss of DoD Contracts – Non-compliance with DFARS, CMMC, or NIST 800-171 could result in contract termination.
* Fines and Legal Penalties – Regulatory bodies can impose hefty fines for failing to meet compliance requirements.
* Reputational Damage – Cybersecurity lapses can erode trust with the DoD, reducing future business opportunities.
* Increased Cyber Risk – Lapses in compliance expose Tantalum Defense Technologies to a higher likelihood of data breaches and cyberattacks.

**Conclusion**

Tantalum Defense Technologies operates within a high-risk environment where cyber threats are increasingly sophisticated and persistent. Given the nature of its work as a DoD cloud services provider, the company is a prime target for cybercriminals, nation-state actors, and insider threats. Without an internal DFIR team, the company risks prolonged downtime, financial losses, regulatory penalties, and compromised national security.

This report has demonstrated that cybersecurity incidents are not a matter of if, but when. As evidenced by past breaches in the defense industry, organizations must be proactive in developing robust incident response mechanisms to detect, contain, and remediate threats efficiently. By establishing a well-equipped internal DFIR team, Tantalum Defense Technologies can reduce its response time to security incidents, ensure compliance with stringent DoD cybersecurity regulations, and protect its mission-critical cloud services.

The financial investment in an internal DFIR team is justified by the long-term cost savings and risk mitigation benefits. The ability to respond swiftly to security incidents, maintain operational resilience, and uphold contractual obligations with the DoD will solidify Tantalum Defense Technologies' reputation as a trusted defense contractor.

The dynamic nature of cyber threats means that Tantalum Defense Technologies must remain vigilant and adaptable to emerging risks. Cyber adversaries are continuously evolving their attack techniques, making it imperative that the organization not only responds effectively to incidents but also proactively enhances its security posture. An internal DFIR team provides the necessary agility to investigate threats, contain breaches, and recover swiftly, ensuring that operations remain uninterrupted.

By integrating advanced threat intelligence, continuous monitoring, and DoD-aligned security practices, Tantalum Defense Technologies can stay ahead of potential attacks. The key to long-term resilience lies in fostering a culture of cybersecurity awareness, investing in innovative defense technologies, and maintaining a robust incident response framework. As the landscape of cyber warfare continues to shift, a proactive and well-equipped DFIR team will serve as the foundation for maintaining national security and securing DoD cloud operations.

**References**

CISA. (n.d.). CISA Cyber Threat Reports. Retrieved from www.cisa.gov

CISA. (n.d.). Cybersecurity Maturity Model Certification (CMMC).

DFARS. (n.d.). DFARS Cybersecurity Requirements. Retrieved from https://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm

Digital Responder. (2020, May). Managing Spend for digital Forensic and Incident Response Services. Retrieved from https://safe.menlosecurity.com/doc/docview/viewer/docN5045123DC2D1f0ade524d642b1805b4b473831e43939b10d35b035943c22e0ddc4aeb7c71f04

DISA. (2018). Cloud Computing Security Requirements Guide (CC SRG).

IBM. (n.d.). What is Digital Forensics and Incident Response (DFIR). Retrieved from https://www.ibm.com/think/topics/dfir

Kerner, S. (2023, November 3). SolarWinds hack explained: Everything you need to know. Retrieved from https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know

MITRE ATT&CK Framework. (n.d.). Retrieved from MITRE: https://attack.mitre.org/

NIST. (n.d.). NIST SP 800-71 Protecting Controlled Unclassified Information (CUI).

SANS. (2024, July 25). The Ultimate Guide to Getting Started in DFIR. Retrieved from https://www.sans.org/white-papers/ultimate-guide-getting-started-digital-forensics-incident-response/

The New York Times. (2011). Stolen Data is Tracked to Hacking at Lockheed. 2.

The New York Times. (2018). Boeing Hit by 'WannaCry' Malware Attack.

U.S. Government. (2013). Federal Information Security Amendments Act.