Critical Infrastructure Protection (CIP) - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2025 - 2030)

Market Report | 2025-04-28 | 174 pages | Mordor Intelligence

AVAILABLE LICENSES:

- Single User License $4750.00
- Team License (1-7 Users) $5250.00
- Site License $6500.00
- Corporate License $8750.00

Report description:

The Critical Infrastructure Protection Market size is estimated at USD 154.32 billion in 2025, and is expected to reach USD 187.03 billion by 2030, at a CAGR of 3.92% during the forecast period (2025-2030).

The critical infrastructure protection (CIP) market is growing as it plays an active and dynamic part in helping modern society's seamless progression and assimilation. The performance, safety, reliability, continuous operation, maintenance, and protection of critical infrastructure are national priorities across the globe.

Key Highlights
- Critical infrastructure (CI) offers essential services that underpin society and serve as the spine of any nation's economy, health, and security. The power used in homes and industries, transportation, and communication systems is a part of critical infrastructure.
- Due to rapid urbanization worldwide, there has been immense stress on city infrastructure, and governments are focusing on enhancing the infrastructure, such as transport, energy, and water, to provide better livability. The information and the telecommunications sector also play a crucial role in the market.
- Furthermore, various critical infrastructure and operational technologies widely support defense bases and facilities, from power generation and utilities to building automation and security systems. Destruction of these bases can weaken national economic security, such as loss of power, exposure of confidential information, interruptions to operations, etc. Therefore, the issue of critical infrastructure protection is emerging as a primary concern for governments, infrastructure managers, and local authorities. The European Union (EU), through its European Program for Critical Infrastructure Protection (EPCIP), announced the significance of CIP to all its member states and citizens.
- Industrial control system devices play an essential role in critical infrastructures, such as the power grid. In recent years, various

ICS devices have been accessible online, resulting in potential security issues. However, there is a lack of deep understanding of the characteristics of these devices in cyberspace. A lack of standard-based technical security testing puts the industrial control environments and critical national infrastructure at risk of cyberattacks.
- Post-COVID, with more people working remotely, there was a surge in cyber threats, including phishing attacks and ransomware. Critical infrastructure operators faced an increased risk of cyber-attacks as they adapted to new working conditions that might not have been as secure as their traditional setups. This has lead to major market growth post pandemic.

Critical Infrastructure Protection (CIP) Market Trends

Maintenance and Support Services to Witness Major Growth

- Maintenance and support services are a set of procedures designed to ensure the performance of the service for business continuity. These services include maintenance of hardware and software systems on a regular basis. Maintenance of critical infrastructure is essential for continuous operation. Damage to a critical infrastructure may have a significant negative impact; therefore, business development managers and owners of critical infrastructure are investing significantly to protect the core of business operations and critical security-related areas of the organization.
- Unlike IT networks, the lifetimes of operational technology (OT) components are in the range of decades, varying from 15 to 25 years, and these systems become an easy target for cyberattacks because of the vulnerabilities and holes in such outdated software and hardware. Therefore, they need to be maintained regularly.
- Energy and power generation and distribution networks are observing a growing demand for maintenance and support services to keep pace with dramatically increasing electricity demand. The energy sector is uniquely critical because it enables all other critical infrastructure sectors. Without reliable and secure electricity networks, economies and communities cannot function. This has increased the importance of cybersecurity for energy and utility companies because they face the challenges of protecting vast supply chains, electricity grids, and customer information from cyber threats.
- In October 2023, Google Cloud joined the E-ISAC Vendor Affiliate Program to contribute to the electricity industry's collective defense by providing subject matter expertise on critical vulnerabilities and security solutions. As a Vendor Affiliate Program partner, Google Cloud will devote experts to working alongside industry leaders to transform and secure the electricity sector. The company will bring the Google Cybersecurity Action Team to protect the electricity industry against cyberattacks. Google has also committed to investing at least USD 10 billion over five years to advance cybersecurity.
- Overall, the growing collaboration between industry and vendors for the maintenance and support of supply chain interdependencies and strengthening their collective defense against growing cyberattacks that include ransomware, supply chain compromise, botnets, and worm attacks to protect critical infrastructure is propelling the segment growth in the market studied.

North America is Expected to Hold Significant Market Share

- The adoption of critical infrastructure protection (CIP) in the United States has been a comprehensive and evolving process driven by the need to secure vital systems and assets, ensuring national security.
- In the energy sector, regulatory bodies like the Federal Energy Regulatory Commission (FERC) enforce standards to ensure the security of power grids and energy infrastructure. The increasing digitization of power grids and utilities necessitates a strong focus on cybersecurity. The Department of Homeland Security (DHS) and the Cybersecurity and Infrastructure Security Agency (CISA) play vital roles in protecting these systems from cyber threats.
- The United States electricity segment contains more than 6,413 power plants with approximately 1,075 gigawatts of installed generation. The energy and power industry across the United States is experiencing a significant uptake of RADAR security

technologies to safeguard critical assets. Concerns regarding the economy, public safety, operational continuity, and environmental well-being have elevated cybersecurity as a foremost priority for power and utility companies.
- Smart cities and transportation systems heavily rely on digital technologies, which expose them to cyberattacks. CIP develops robust cybersecurity strategies and threat intelligence to mitigate these risks. The transportation sector falls under the purview of the Department of Transportation (DoT), which enforces regulations for securing transportation infrastructure, including airports and mass transit systems.
- The Department of Transportation is leading federal initiatives to revamp the country's infrastructure. They have a major focus on integrating cybersecurity through significant investments under the Bipartisan Infrastructure Law. This endeavor primarily takes place at the state and local levels. Moreover, in May 2023, Illinois Tech's initiatives received a USD 10 million federal grant to establish a new Tier 1 transportation center, further strengthening cybersecurity in navigation systems.
- In March 2023, the Federal Bureau of Investigation (FBI) published a report. It stated that in the previous year, the FBI received reports of ransomware attacks across the country, with more than one-third affecting organizations in the critical infrastructure sectors. Out of the 2,385 ransomware incidents reported, 870 targeted critical infrastructure entities. The high incidence of ransomware attacks targeting critical infrastructure sectors underscores the need for robust critical infrastructure protection measures. In reference to this, in May 2023, the US Cybersecurity & Infrastructure Security Agency (CISA) launched the Ransomware Vulnerability Warning Pilot (RVWP) program to help secure critical infrastructure organizations to protect their systems from ransomware attacks.
- The Canadian Government, primarily through Public Safety Canada, has been actively engaged in coordinating and enhancing critical infrastructure protection. With the increasing importance of digital infrastructure, Canada has been concentrating on enhancing cyber security for critical systems. This includes regulations and standards to safeguard against cyber threats.
- As per the Canadian Government, ransomware is almost certainly the primary cyber threat to the reliable supply of oil and gas to Canadians, and the most likely targets for cyber threat actors intending to disrupt the oil and gas supply in Canada are bottlenecks in the oil transmission and processing stages. Potential targets include large-diameter pipelines' business and OT networks, transfer terminals, and major refining facilities.

Critical Infrastructure Protection (CIP) Market Overview

The Critical Infrastructure Protection Market is highly fragmented, with the presence of major players Bae Systems PLC, Honeywell International Inc., Airbus SE, Hexagon AB, and General Electric Company. Players in the market are adopting strategies such as partnerships and acquisitions to enhance their product offerings and gain sustainable competitive advantage.

- September 2023 - Ericsson announced an expansion of its successful and long-standing partnership with Google Cloud to develop an Ericsson Cloud RAN solution on Google Distributed Cloud (GDC) that offers integrated automation and orchestration and leverages AI/ML for additional communications service providers (CSP) benefits. GDC is a fully managed hardware and software portfolio that extends Google Cloud's infrastructure and services to the edge and into the data centers. Deploying Ericsson Cloud RAN on GDC Edge enables the delivery of a fully automated and very large-scale distributed cloud, resulting in an efficient, reliable, highly performant, and secured software-centric radio access network infrastructure.
- June 2023 - McAfee Corp., a global player in online protection, announced McAfee Business Protection, a new comprehensive security solution for small business owners in collaboration with Dell Technologies. McAfee Business Protection helps Dell small business customers avoid cyber threats and vulnerabilities with award-winning security, identity and dark web data monitoring, VPN, web protection for safe browsing, and more.

Additional Benefits:

- The market estimate (ME) sheet in Excel format
- 3 months of analyst support

Table of Contents:

SCOTTS INTERNATIONAL

Critical Infrastructure Protection (CIP) - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2025 - 2030)

Market Report | 2025-04-28 | 174 pages | Mordor Intelligence

To place an Order with Scotts International:

- - Print this form
- - Complete the relevant blank fields and sign
- - Send as a scanned email to support@scotts-international.com

ORDER FORM:

Select license	License	Price
	Single User License	$4750.00
	Team License (1-7 Users)	$5250.00
	Site License	$6500.00
	Corporate License	$8750.00
	VAT	
	Total	

*Please circle the relevant license option. For any questions please contact support@scotts-international.com or 0048 603 394 346.

** VAT will be added at 23% for Polish based companies, individuals and EU based companies who are unable to provide a valid EU Vat Numbers.

Email*		Phone*	
First Name*		Last Name*	
Job title*			
Company Name*		EU Vat / Tax ID / NIP number*	
Address*		City*	
Zip Code*		Country*	
		Date	2025-06-25
		Signature