Critical Infrastructure Protection: Concepts and Continuum
Introduction

Modern life is increasingly reliant on a wide-ranging set of functions, services, systems, and assets, commonly referred to as infrastructures. Today, Governments view several of these infrastructures, such as communications, banking, energy, transportation, and healthcare, as critical, since their disruption, destruction, or loss of integrity can impact a nation’s stability.

Critical infrastructures are often thought of as physical assets. Over the past few decades, however, infrastructures that historically relied on physical assets have integrated information and communications technology (ICT). The resulting improvements in these infrastructures have helped to drive down costs, increase service offerings, and promote economic and social opportunities. The essential nature of infrastructures’ functions and services renders their protection an important national and international policy concern. Unlike traditional security concerns, which could often be mitigated through government or regulatory actions, protecting critical infrastructures, which requires unprecedented coordination, collaboration, and trust.

Understanding critical infrastructure risks and organizing effective protective measures is a complex undertaking that spans public and private organizations, including government agencies, infrastructure owners and operators, and technology vendors.

Providing secure, private, and reliable experiences in the computing ecosystem is central to Microsoft’s vision for its software and services. In 2002, the company established Trustworthy Computing as a top company priority, redefining its mission and strategy in the key areas of security, privacy, reliability, and business practices. And in 2006, Microsoft established a dedicated team of experts, the Global Security Strategy and Diplomacy team, which collaborates with governments, infrastructure owners and operators, and technology vendors to understand and mitigate risks to critical infrastructures by providing leadership, expertise, and guidance on policy and operational challenges.

Microsoft has a unique view of cyberthreats, as each month the company receives threat intelligence from more than 600 million systems in more than 100 countries and regions. In addition, Microsoft works closely with government, enterprise, and consumer customers around the world to assess, manage and respond to risks.

Drawing upon its work with these customers and its global partners, coupled with more than three decades of experience with its own internal systems, Microsoft has found that effective critical infrastructure protection efforts share three core principles:

- Establishing trustworthy policies and plans;
- Building resilient operations; and
- Promoting innovative investments.

These, enabled by trusted collaboration and information sharing, form a continuum for protecting critical infrastructure.
Terms and concepts

Critical infrastructure policy, planning, and operations involve a number of important terms and concepts:

- **Critical infrastructure**: The key systems, services, and functions (IT or physical) whose disruption, destruction, or exploitation could have a debilitating impact on public health and safety, commerce, and national security, or any combination.

- **Critical information infrastructure**: Networks of information and communications technologies (ICT) and data that support, link, and enable critical infrastructure operations, and whose disruption, destruction, or exploitation could have a debilitating impact.

- **Software assurance**: Ensuring that software, hardware, and services are free from intentional and unintentional vulnerabilities and function as intended.

- **Cybersecurity**: The discipline, techniques, and tools that protect the confidentiality, integrity, and availability of information and communications technology and data.

- **Critical infrastructure protection (CIP)**: A continuous process of strategic and operational risk management to improve the security and resiliency of critical infrastructures.

*Figure 1. Relationships between critical infrastructure protection concepts*

Throughout this paper, the term critical infrastructure protection (CIP) is used to include a broad range of interrelated activities, including protection of critical information infrastructure and software assurance.

Communities of participants in critical infrastructure protection efforts are often termed CIP stakeholders. Immediate stakeholders include government agencies, critical infrastructure owners and operators, and technology vendors, while the broader set of stakeholders can include academia, subject matter experts, and international organizations.
Protecting critical infrastructure is a continuum

Critical infrastructure protection (CIP) is not an end state, but a continuous process of managing risk to improve security and resiliency. While countries design and implement CIP programs differently, there are capabilities and functions that are common to most CIP efforts—a set of three interrelated core principles that form a CIP continuum:

- **Establishing trustworthy policies and plans** for protecting critical infrastructure in today’s dynamic environment.
- **Managing risk**: Fostering capabilities for preventing, detecting, responding to, and recovering from risks to promote operational resiliency.
- **Promoting innovation and investments** by learning from policy and operations that can guide the allocation of resources for practices, programs, education, and research related to CIP.

CIP is sometimes viewed narrowly, through basic capabilities for protection, detection, response, and recovery. With this narrow view, however, stakeholders can fail to address the very elements needed to sustain such capabilities over the long term. As a result, understanding the CIP continuum can help stakeholders more effectively deliver both the strategic and operational capabilities needed for protection, detection, response, and recovery.

Additionally, by focusing on CIP as a continuum, stakeholders can better plan for and manage the ongoing lifecycle of CIP, and ensure that stakeholders are sharing lessons learned among key communities in policy, operations, and investments. It is important to note that there is no specific area called *protection*. Rather, protection is the aggregate of these capabilities and functions that, taken as a whole, help reduce risk, increase resiliency, and safeguard the delivery of essential systems, services, and functions.
Trusted collaboration and information sharing ground the CIP continuum

While effective critical infrastructure protection is a constantly evolving, ongoing process, it must be grounded in trusted collaboration, which involves all key stakeholders working together, and information sharing, where information regarding threats and incidents is openly and voluntarily shared through established channels. This enables stakeholders to collaborate across sectors and borders to better manage risks. Each party brings its expertise to the table, and all benefit from one another’s ongoing shared contributions.

By looking at critical infrastructure protection through the lens of the CIP continuum, policy makers in both the public and private sectors are able to undertake the activities and processes necessary for defining goals and achievable objectives; organizing to address challenges; identifying risk assessment and management processes; and establishing mechanisms for reviewing and regularly updating plans and programs.

Managing critical infrastructure risk is an extremely dynamic process. The increased reliance of modern societies on IT means that when issues—such as zero-day exploits—begin to emerge in infrastructures, incidents can develop extremely quickly. As a result, effective policy and operational communities in the realm of CIP today work together closely to rapidly adapt and respond to changes in the threat landscape. This convergence promotes more effective planning and helps pull together the support needed to ensure resilient operations. For example, governments can work with infrastructure owners and operators to better understand national and even transnational risks, and to assist in removing possible impediments to delivering essential services.

Key CIP capabilities

This guide discusses approaches to establishing the three core elements of the CIP continuum outlined above. Specifically, critical infrastructure protection requires that stakeholders—governments, infrastructure owners and operators, and technology vendors—work collaboratively and share information to:

- **Prepare** for a national-level critical infrastructure protection program by identifying key stakeholders and examining the status of existing security programs.
- **Partner** across government and industry through mechanisms that are transparent, cooperative, and clearly defined.
- **Coordinate** CIP operations by defining roles and responsibilities, and establishing mechanisms for coordination.
Plan for long-term readiness by assessing and managing infrastructure risks, developing capabilities to provide response and recovery in the event of disruptions, and investing in research, education, programs, and practices that contribute to long-term security goals.

Prevent potential attacks against critical infrastructures both through sustained governmental leadership and through the use of advanced anticrime technological tools. A large part of risk management is focused on deterring events (that is, decreasing the likelihood that an event will occur), containing events from expanding, and/or preventing events from causing damage if they occur (that is, decreasing their impact).

Detect when an attacker has accessed a network, system, or asset, which requires skilled forensic investigators equipped with cutting-edge tools and resources. Any approach should consider dedicated threat intelligence, continuous monitoring, and strong forensics.

Respond quickly and systematically to critical infrastructure threats and incidents, including through such collaborative mechanisms as round-the-clock computer security incident response teams (CSIRTs).

Recover from an impacting incident by adhering to well-defined and thoroughly tested recovery plans.


Programs. Undertake discrete CIP programs designed to meet specific objectives. Each of these programs has its own lifecycle, maturing and evolving as a result of incidents, events, and perceived threats.

Education. Invest strategically in education and training to create a highly skilled workforce capable of addressing future security challenges. This workforce can then build security capabilities into new products and infrastructures, advancing CIP.

Research. Make strategic long-term investments in security research to meet the evolving critical infrastructure demands of an interconnected world.

Sharing threat information leads to improved CIP

Sharing threat-based information such as vulnerabilities, hacking trend data, new threat identification, or even unexplained anomalies impacting a product or service can enable better protection of critical systems and response to emerging issues. This can also help lead to new protections or mitigations, sometimes even before any impact. If done widely and efficiently, sharing threat information removes the head start afforded to an early discoverer and prevents the exploitation of security vulnerabilities.

However, for threat-information sharing to be successful, it must be focused on new and novel threats, and not just known issues that already have remediations. A program to share threat information must also be coordinated by a strong and competent national computer emergency
readiness team with authority to share threat information with key stakeholders in the government, private sector, and in some instances the broader public.

They also need to be able to involve law enforcement where needed (for example, to help seize a machine controlling a botnet), while simultaneously respecting privacy and civil liberties with adequate judicial oversight and enforcement of privacy protections.

There have been many discussions about the appropriate level of information shared between private sector entities looking to respond to vulnerabilities or threats, and between those private sector entities and government agencies. It is important that a national strategy emphasize that whether or not information about threats is passing between private sector partners or to a government agency, the system design must consider privacy at the outset. Privacy-by-design principles must also be applied to help mitigate privacy risks regardless of the type of data shared.

Ensuring adequate judicial oversight and enforcement of privacy protections also becomes increasingly important, as well as a clear understanding of privacy requirements so essential to a capability for sharing threat information. Threat and vulnerability warning procedures and practices must fit privacy protections within individual countries, but also recognize that at times warnings and alerts must be sent across borders.
Establishing trustworthy policies and plans

Trustworthy policies and plans are the foundation for building and maintaining CIP programs. There are four fundamental capabilities that are integral to building trustworthy policies and plans: preparing, partnering, organizing, and planning.

Prepare

To establish a national-level CIP program or review an existing one, it is important to first understand the scope and status of existing policies and security programs, as well as identify existing operational capabilities.

Review policies and existing programs

A policy review will help determine what policies, authorities, organizations, and capabilities are currently in place, and what gaps, if any, exist. To create a thorough understanding of the landscape, it is also important to examine a range of policies from law enforcement, national defense, emergency response, and communications.

Taking time to understand the state of security of government systems and their current challenges allows a government to demonstrate its commitment to security by first taking corrective actions for its systems, if needed, and have a more informed discussion with critical infrastructure owners and operators about current enterprise challenges.

Identify operational responsibilities

For more effective planning, it helps to gain a thorough understanding of existing operational capabilities, beginning within the government, and eventually expanding to critical infrastructure owners and operators and technology vendors. For example:

- Is there a designated emergency management agency or lead within the government?
- Is there a national computer security incident response team (CSIRT) in place?
- Are these two functions related, and to what extent do they coordinate with critical infrastructure owners and operators and technology vendors?
- Are there emergency communications capabilities that connect key governmental and non-governmental decision makers during a crisis?
Partner

Public-private partnerships are a cornerstone of effectively protecting critical infrastructure and managing security risks in both the short- and long-term. Establishing sustainable partnerships requires that all of the participating stakeholders have a clear understanding of the goals of the partnership and the mutual security benefits they will inherit in working together. Although governmental and non-governmental CIP stakeholders often see different value propositions when they collaborate on these challenges, both can benefit when they:

• Establish effective coordinating structures and information-sharing processes and protocols
• Recognize changes in the threat landscape and improve security planning
• Identify and exchange ideas, approaches, and best practices for improving security
• Raise awareness about the importance of CIP and creating an environment for success
• Improve international coordination

Effective partnerships include a range of stakeholders that represent the diversity of the infrastructures themselves. Identifying stakeholders can take time and effort, but it is necessary to ensure that different perspectives, operating conditions, and challenges are considered. Of course, once established, partnerships must be preserved and maintained. Annual reviews or check-ins provide excellent opportunities to ensure that objectives and expectations are being met and, if they are not, to make appropriate corrections.

Coordinate

An effective and efficient CIP program requires that stakeholders have clearly defined roles and responsibilities and establish a coordination mechanism for managing ongoing issues. Critical infrastructures, which can have very complex technical operations, are often not owned or controlled by the government, and CIP efforts generally exceed the capabilities and mandate of any single agency in a government. For example, agencies responsible for defense, law enforcement, communications, energy, transportation, banking, healthcare, and public safety all have important roles in CIP, yet they do not have end-to-end ownership or accountability. For this reason, appointing an overall coordinator, such as an interagency committee, can greatly assist in efforts to protect critical infrastructure.
<table>
<thead>
<tr>
<th>Potential CIP Organizational Models</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>National CIP coordinator</td>
<td>The country's leader appoints an overall coordinator who reports directly to the executive office and has both the political and financial support to organize efforts across government entities and to interface with the private sector.</td>
</tr>
<tr>
<td>Interagency committee or coordinating council</td>
<td>The country's leader appoints a committee or coordinating council from among the key government agencies responsible for information and communications, including commerce, justice and law enforcement, national defense, energy, transportation, finance, and emergency response.</td>
</tr>
<tr>
<td>Government program with incentives for private sector participants</td>
<td>The government establishes and funds a government-wide program that is designed to provide resources and expertise to other government agencies that are increasing efforts to improve security. This same program can support non-governmental CIP efforts by identifying and providing incentives for protecting critical infrastructure.</td>
</tr>
<tr>
<td>Self-regulatory organizations</td>
<td>Critical infrastructure sectors establish their own self-regulatory entities to enhance security and resiliency across their shared operational dependencies.</td>
</tr>
</tbody>
</table>

Organizing CIP roles and responsibilities in the private sector can also take several different forms. Infrastructure owners and operators and technology vendors often form separate policy and operational organizations to respond to CIP challenges. Policy groups generally engage with government counterparts to address planning and regulatory matters, whereas operational organizations tend to engage on technical issues, such as responding to and managing cyberattacks or physical disruptions.

Designating key points of contact for both governmental and non-governmental stakeholders is essential to creating a successful CIP organizational structure. Once these points of contact are identified, a nation can more effectively coordinate its planning activities.
Plan

A CIP plan provides an important framework for organizing various activities related to assessing and managing infrastructure risks; developing capabilities for response and recovery should disruptions occur; and investing in research, education, programs, and practices that contribute to long-term security goals. The planning process is a unique opportunity to build consensus around CIP goals and to increase recognition of its importance to public health and safety, the economy, and defense.

A CIP plan documents the goals of the program and the particular roles of stakeholders in such a way that all can work collaboratively to meet the needs of a nation, specifically:

• Establish clear and achievable goals.
• Identify roles and responsibilities of key stakeholders.
• Create collaborative processes to manage risk that involve critical infrastructure owners and operators and technology vendors.
• Underscore the importance of an all-hazards (physical, cyber, natural, and man-made) approach to risk management.
• Outline key operational needs.
• Establish a process for reviewing and updating these plans.
• Ensure that there is transparency and accountability.
• Identify performance measures.
Managing risk

The goal of risk management is not to eliminate all risk but rather to mitigate, transfer, or accept risk through organizational, technical, and programmatic efforts that are supported and sustained through company-wide risk-management offices and programs.

Risk management starts with a top-down approach that begins with an assessment of the entirety of an information and communications infrastructure, and then defines assets in physical terms and in terms of critical functions. Stakeholders then organize risk-reduction efforts around prevention, detection, response, and recovery to build robust, sustainable, and repeatable processes for improving the security of critical infrastructures.

An Enterprise Risk Management (ERM) Program can provide insight into the most significant short- and long-term risks to critical infrastructure, ensure accountability and management of those risks, and facilitate a global and programmatic approach to risk management. An effective ERM program can help inform risk owners about what preventive controls to invest in and tracks the effectiveness of those controls over time, providing constant feedback and insight into the state of risk.

Prevent

A large part of risk management is deterring or discouraging potential attacks against critical infrastructures—that is, decreasing the likelihood that an attack will occur—both through sustained governmental leadership (including by national defense and law enforcement agencies) and through the use of advanced anti-crime technological tools. In addition, managing risk includes containing events from expanding, and preventing them from causing damage if they occur (that is, decreasing their impact). Doing some combination of all of these mitigates the risk.

Through prevention enterprises should be able to track risks and report them to the right level in a company, with the most significant risks being made known to the board of directors. It is important to include the following elements in any risk analysis:

- Changes in the risk drivers or scenarios within a risk area
- Progress since the last update, such as risk mitigation or improvements in controls
- Changes in direction or timing for reduction or mitigation, such as milestone changes
- Risk ownership and support from the responsible organizations, such as changes due to reorganizations
- Related high-risk audit issues that are open or pending
Detect

Microsoft uses a multi-layered approach to detecting cyberincidents, with responsibility spread among the business units across the company. Data is collected from systems and devices using common industry tools and standards, through well-known Microsoft products or security organizations, as well as through Microsoft's own internal processes and technologies. That data is then analyzed by the teams that administer the environments to detect isolated incidents, and by a centralized group that looks for attacks against multiple business groups or advanced attacks by determined adversaries. Microsoft's privacy practices, the applicable privacy statements, and relevant regulatory or contractual requirements provide a framework to help ensure that the data is appropriately handled.

Detection may be the most critical of the four risk-management areas. Talented and patient adversaries will delete logs, change data, and take whatever actions are necessary to gain and retain access to a network. So detecting when an attacker has accessed a network, system, or asset requires incredibly skilled forensic investigators equipped with cutting-edge tools and resources. Any approach to detection should consider:

- **Dedicated threat intelligence.** To defend a critical infrastructure against targeted attacks, companies must have internal teams who have the skills necessary to develop, use, and manage threat intelligence.

- **Continuous monitoring** ensures that adequate data will be available to determine whether a compromise has occurred. Monitoring services should be divided into three categories:
  - Baseline security monitoring for broad detection of malicious or anomalous network activity
  - Specialized security monitoring for critical assets and critical processes
  - Data analysis and reporting to provide telemetry to key internal security detection and response partners across the enterprise

If an anomaly is detected and triaged, the detection process should then transition into an established and defined process to respond to the incident.

- **Strong forensic skills and tools.** It is absolutely essential to find personnel who have strong forensic skills and provide them with the tools and technologies that enable continuous monitoring and threat intelligence. If an attack is promulgated by a nation state, and is thoughtful and well-resourced, then the forensic team tasked with uncovering such a compromise must be similarly skilled and be able to draw on strong technological resources.
Respond

Microsoft recommends the Incident Command System as a strong foundation for any response system. It has an established history of success in the United States, and takes a well-recognized approach that:

- Allows for the integration of facilities, equipment, personnel, procedures, and communications operating within a common organizational structure.
- Enables a coordinated response among various jurisdictions and functional agencies, both public and private.
- Establishes common processes for planning and managing resources.

Clearly, incident response is a priority for all IT companies, given the ways in which attackers attempt to use vulnerabilities in software or compromise features in a product or service to do harm.

When a company is assessing whether a vulnerability merits activating an incident response process, that process should reflect the draft international standards on Vulnerability Handling (ISO/IEC 30111) and Vulnerability Disclosure (ISO/IEC 29147). This may also include creating a Common Vulnerabilities and Exposures identifier, and taking steps to assess the severity and exploitability of the vulnerability.

Recover

An organization’s ability to recover from a cybersecurity incident is largely dependent on its overall capabilities for reliability and resiliency. For example, at Microsoft, reliability means more than simply making dependable software and services. It also means investments in processes and technology to improve reliability, a continuing focus on every customer’s experience, and active partnerships with a wide variety of software and hardware companies.

Traditional enterprises and cloud services are managed with a focus on avoiding service failures. However, the scale and complexity of the modern enterprise, including cloud services, bring inherently different reliability challenges than were faced by the enterprises or hosted services of the past. Despite the best plans and detailed risk-management efforts, hardware will fail, people will make mistakes, and software will contain vulnerabilities. Therefore, those protecting critical infrastructures should develop appropriate strategies and plans to account for the recovery of key assets and resources (downtime within a specified and appropriate window), and their resiliency (no downtime).
Those managing business continuity should consider the following standards: BS25999, ISO 22301, ISO22399, and NFPA1600. These will help ensure timely, relevant, and accurate operational information by specifying processes, systems of work, data capture, and management. Although these standards provide a solid grounding, businesses will nevertheless face challenges that cannot be anticipated. Efforts to address them are overseen by an effective Enterprise Business Continuity Management (EBCM) program.

The primary objective of an EBCM program should be to ensure the existence of effective, reliable, well-tested recovery and resiliency processes, systems, plans, and teams that can be counted on during an event to support the continuity of business operations and to minimize adverse impacts. The EBCM program should take an all-hazards approach that includes cybersecurity to help leadership in identifying, managing, and tracking business continuity risks throughout the company.

From an operational standpoint, there are certain specific principles and practices to keep in mind when thinking about recovery:

- **Design for recoverability.** Teams should be able to restore a service or its components quickly and completely if a service interruption occurs. For example, the organization should design the service for component redundancy and data failover so when failure is detected, the service automatically uses another component or physical location to keep the service running.

- **Diagnostic aids** must be suitable for use in non-production and production environments, and should rapidly detect the presence of failures and identify and analyze their root causes using automated techniques.

- **Automated rollback.** To help mitigate the impact of mistakes, systems should provide automated rollback for most aspects of operations, from system configuration and application management to hardware and software upgrades.

- **A defense-in-depth approach** helps to ensure that a failure remains contained if the first layer of protection does not isolate it. In other words, organizations should not rely on a single protective measure, but rather factor multiple protective measures into their service design.
Promoting innovation and investment

The security systems that protect critical infrastructure must constantly evolve to counter ever-more sophisticated threats. People, processes, and technology must all be considered when outlining the CIP practices, programs, education and training, and research needed to secure critical infrastructures today and in the future.

All stakeholders can make important contributions to innovation in protecting critical infrastructure.

• For operators, these innovations may involve updating practices for managing risk, collaborating with vendors on emerging threats, and improving line of business applications, security operations, and incident response.

• Leading technology vendors may invest in research on emerging cybersecurity threats as well as in improving their software development processes, security features, and products.

• Governments can make investments in infrastructures, such as developing mechanisms to support secure collaboration among disparate organizations that include vendor-neutral information sharing. They can also strengthen education and training programs for relevant stakeholders, and fund basic research and development.

Practices

Identifying, developing, and refining practices and procedures is an important and often overlooked investment in protecting critical infrastructures. Like all capabilities of the CIP continuum, practices must continually be revised and updated. Similarly, identifying and sharing best practices among CIP stakeholders builds trust and advances the security of systems and processes.

The exchange of best practices can take many different forms. Industry- or government-sponsored events often provide for an exchange of information about practices that have proven to be effective. This type of broad public exchange is often best suited to overarching topics, such as risk management. More specialized practices, on the other hand, are best shared among specific communities of interest. For example, energy and communications providers and information technology vendors are more likely to exchange data amongst themselves in small groups. Similarly, law enforcement and IT vendors may work together on a bilateral or multilateral basis to share insights on cyberforensics.
Identifying, sharing, and implementing innovative practices are valuable and cost-effective means for improving security. As a result, CIP efforts should ensure that there are processes in place that serve to continually innovate and maintain the agility of practices within the overall CIP continuum.

**Programs**

CIP efforts generally comprise discrete programs designed to meet specific objectives. For example, governments commonly establish programs to address information security within specific departments and agencies. Other CIP programs may include efforts to create interfaces with the various elements of a critical infrastructure, as well as CSIRTs, cybercrime investigation centers, joint industry and government coordination centers, or risk-management efforts. Each of these programs has its own lifecycle, maturing and evolving as a result of incidents, events, and the constantly changing nature of cyberthreats threats. The requirements and resource needs of these programs are guided by information sharing and collaboration between the policy and operational activities of the CIP continuum.

**Education**

Education and training are among the most strategic investments that can be made to advance critical infrastructure protection. These investments can develop the highly skilled workforce needed to capably address future security challenges. Building upon research investments, these advancements must be delivered to students and practitioners in both IT and operations. College curricula should be updated to ensure that computer scientists and engineers have a solid foundation in security knowledge. Such a foundation will enable the developers of tomorrow to build security capabilities into the products and infrastructures they design. Accordingly, related management disciplines must possess a keen understanding of the threat environment and of risk-management practices.

The educational background required to successfully defend against current threats does not stem only from academic institutions, however. Governments, infrastructure operators, and vendors should all deliver updated training on a regular basis to their employees, partners, and customers.
Research

To meet the increased demands of today’s interconnected world, strategic, long-term investments must be made in security research for critical infrastructure, specifically in the following areas:

- New computing paradigms are game-changing for security. Social, peer–to-peer, and cloud-based computing are driving the technology industry in ways that challenge traditional thinking about security and privacy. New thinking about robust networks, as well as formalized descriptions of confidentiality and integrity, are needed to frame the design and analysis of modern secure systems.

- Signature-based detection must be augmented with robust heuristics for detecting and mitigating zero-day attacks.

- Metrics that quantify important aspects of security could facilitate security decision-making and risk management. Data throughout all phases of the development lifecycle needs to be cataloged, assessed, and used to provide metrics that guide the decision-making process, including day-to-day development guidance and release readiness measures.

- Code and binary-level analysis currently allows reasoning about a small subset of security issues. An order of magnitude improvement in the capability to analyze source and binary code for potential design defects must be sought. A better understanding of patterns of insecurity and how those patterns can be found in code and binaries would be of help in meeting this goal.

- Software architectures and designs that improve assurance of secure code would lead to more widespread secure development and reduce the risk of insecure deployment. Recommended architectures and designs would lead to the development of secure reusable components and put secure development within the reach of a larger number of software developers.
Summary

Sustained efforts around policy, operations, and investment are central to the level of readiness required to protect critical infrastructure. These efforts, in turn, are grounded in trusted collaboration and information sharing among all key stakeholders—governments, infrastructure owners and operators, and technology vendors. Trusted collaboration means that each party brings its expertise to the table, and all benefit from one another’s continuous, shared contributions. Sharing useful information in turn facilitates collaboration and enables stakeholders to better manage risk within and across sectors and borders. Stakeholders can then successfully implement the capabilities of the CIP continuum as listed on page 6.

Critical infrastructure protection (CIP) is not an end state, but a continuous process of managing risk to improve security and resiliency. While countries design and implement CIP programs differently, there are three core principles that are common to the continuum of most CIP efforts:

• Establishing transparent policies, plans, and programs for critical infrastructure protection in today’s dynamic environment.

• Fostering capabilities for identifying, managing, and mitigating risks to promote operational resiliency.

• Promoting innovation and investments by learning from policy and operations to guide the allocation of resources for practices, programs, education, and research related to CIP.

While every critical infrastructure is unique, the CIP continuum outlined in this document can provide a framework for analyzing risk and gauging readiness for addressing it. Stakeholders can and must contribute to evaluating and strengthening that readiness, not just at the inception of critical infrastructure but throughout its lifecycle.

Microsoft Global Security Strategy and Diplomacy

In December 2006, Microsoft formed this dedicated team of experts to better address the unique challenges faced in protecting critical infrastructure. The company’s goal is to enhance critical infrastructure security by increasing the trustworthiness of software and services, and by collaborating with governments and critical infrastructure providers to reduce and manage risks.

For more information on Microsoft’s Global Security Strategy and Diplomacy team, or its critical infrastructure protection work, visit www.microsoft.com/cybersecurity or contact the team at cyber@microsoft.com.

© 2014 Microsoft Corporation. All rights reserved.

This document is provided "as-is." Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it. This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.