Solutions to Protect **Critical Information Infrastructure** in India

Secure your infrastructure and achieve attack surface visibility

NOVEMBER 2016

SKYBOX™
SECURITY

Copyright © 2016 Skybox Security, Inc. All rights reserved. Skybox is a trademark of Skybox Security, Inc.
All other registered or unregistered trademarks are the sole property of their respective owners.

Contents

Overview

Cybercriminals are becoming increasingly sophisticated and persistent, and the networks and infrastructure that they're attacking need to evolve to withstand these continuous threats. As an integral part of this evolution process, organizations need to shift strategies for addressing threat exposures from a reactive to a proactive position. This includes building more resilient networks, reducing their attack surface and remediating vulnerabilities exposed to attackers. A successful adaptation to this approach is critical as commerce and society at large rely on information stored and transmitted on the networks linking India with the rest of the world.

To provide guidance, the government of India has established controls for the architecture, maintenance and ongoing development of critical information infrastructure (CII) for its government and commercial entities. The National Critical Information Infrastructure Protection Centre (NCIIPC) laid out 40 tenets clearly defining CII and prescribing foundational methods to ensure that these systems are protected.[1]

At its heart, the NCIIPC's mission is, "to take all necessary measures to facilitate protection of Critical Information Infrastructure from unauthorized access, modification, use, disclosure, disruption, incapacitation or destruction through coherent coordination, synergy and raising information security awareness among all stakeholders."

The overarching goal of the NCIIPC guidelines is to help provide a framework for organizations to create resilient information infrastructure that can withstand modern, repeated cyberattacks. The NCIIPC's guidelines apply to any network or link between networks that can create an exposure to critical systems that support the day-to-day operations of commerce and government.

The NCIIPC specifies the industries of electricity, telecommunications, banking, rail, national defense and air traffic as critical areas of the economy that should adhere to and implement the recommended guidelines to create a resilient architecture. While the guidelines are fairly rigid, they are designed to complement industry best practices for network security that an organization should already have in place.

NCIIPC security requirements and guidelines span physical and virtual security, vulnerabilities, application development, testing and incident preparation and response. They are designed to improve security postures and reduce the attack surface. Achieving and maintaining NCIIPC compliance presents a challenging but not impossible task.

[1] Guidelines for Protection of National Critical Inforamtion Infrastructure: http://ow.ly/Wfp5306jGgQ

Challenges

The industries that fall under critical infrastructure attract hackers for different reasons. Banking and financial services companies can hold troves of financial information that can be resold to the highest bidder on the black market and "dark web." Industrial control system (ICS) and supervisory controls and data acquisition (SCADA) environments that regulate production on assembly lines, energy fields and gas and oil pipelines are attractive to corporate spies, hackers and even foreign, state–sponsored threats. Once these threats enter an organization through a vulnerable system, access point or remote sensor, the damage that can be done to the system, customers, worker safety and the environment is almost immeasurable.

But using the guidelines prescribed by NCIIPC, organizations have a framework for the architecture and best practices to create a security program that systematically reduces their attack surface.

Understanding the true nature, size and perimeter of an organization's attack surface is the first step to securing the infrastructure that supports the flow of data and sensitive or critical information. Modern cybercriminals are not school-age hackers scanning for open ports on internet servers; these criminals are organized — sometimes even state-sponsored — and have a growing number of tools at their disposal to infiltrate an organization and exfiltrate data in secret.

Visibility into the network and the risks it faces is necessary for a complete picture of all the ways that an organization is exposed to attacks. Once this is assessed, the next step is to implement programs to manage it. These programs need to provide IT and security staff with intelligence and analytics to ensure that the organization is protected in the era of continuous compromise.

A frequently used approach to safeguard many CII control elements is to model an organization's network to understand the perimeter and exposures to potential attacks, then secure the data within the network to prevent malware and internal data loss.

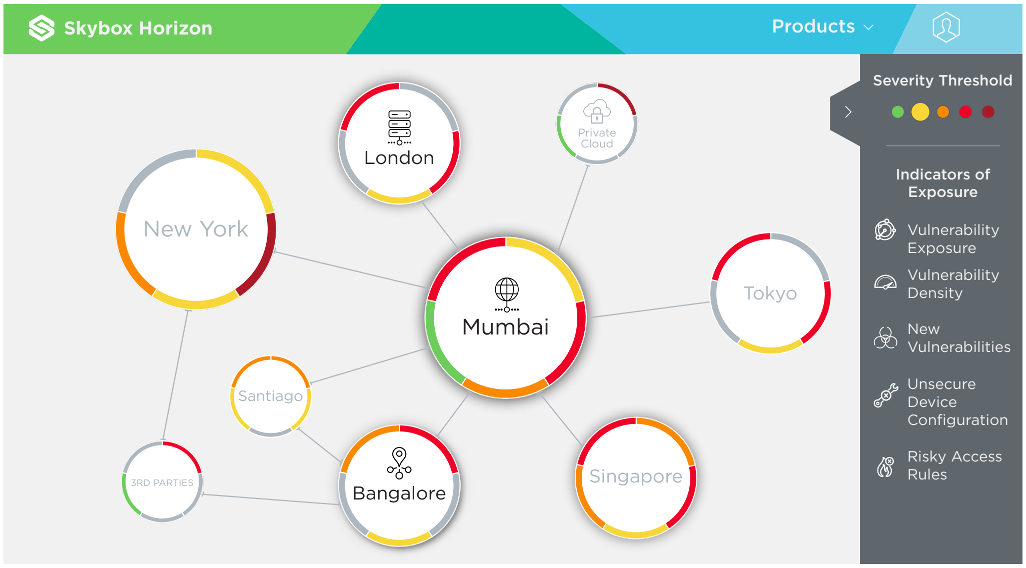


FIGURE 1: A map showing geographical sites within an attack surface and the paths between them. The map provides an at–a–glance view of IOE severity at each site.

Solutions

To begin to address these challenges, an organization needs to create a complete model of their network. As such, this model should include all network devices such as routers, switches, load balancers, firewalls and intrusion prevention systems (IPSs), as well as the various connections within the network. Path analysis of the various ways that data interacts with and traverses the network is the important next step. Understanding how and where certain users can move about the network provides a deep understanding of security architectures and controls.

Skybox® Security empowers security managers to automatically turn vast amounts of complex data into context-aware, prioritized actions, even on the scale of enterprise security management. Powerful security analytics software combined with modeling, simulation and intelligent automation gives context to an IT environment, improves business services and helps organizations immediately respond to threats.

Using the Skybox platform for both security policy management and vulnerability and threat management eases the burden of complying with the guidelines and recommendations of the NCIIPC, and provides focus and direction for the staff that is responsible for managing the security of CII.

Skybox creates a comprehensive picture of the IT infrastructure for the organization (on premise and in the cloud), including all the security controls and indicators of exposure (IOEs), such as new, exposed or concentrations of vulnerabilities, unsecure device configurations and risky access rules.

The Skybox® Security Suite helps organizations implement 13 of the 40 controls for CII (see Table 1: NCIIPC Requirements and Skybox); this integrated security platform focuses on many of the components of the CII controls that deal with securing and remediating vulnerabilities, network access and routing and the hardening of security controls.

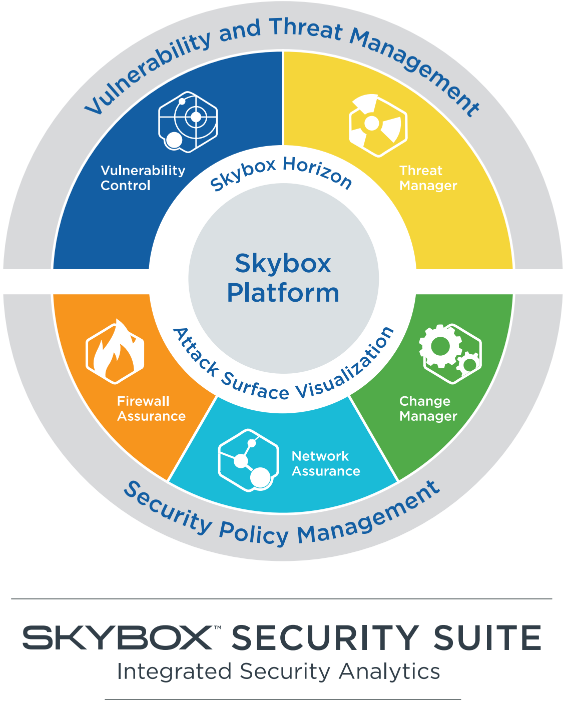


FIGURE 2: The Skybox Security Suite is comprised of five modules and an attack surface visualization solution on a common platofrm addressing complex security issues in vulnerability and threat management and security policy management

Fulfilling the Requirements

With 40 requirements, maintaining CII without advanced tools can be overwhelming. Skybox automates many of the processes needed to fulfill the requirements, facilitates collaboration and provides vital intelligence to compliance management teams. Skybox helps security practitioners examine and extract more value from both the processes and technology already in place to secure their attack surface and maintain compliance with the NCIIPC requirements — even as the network, team and technology evolves.

PROCESSES

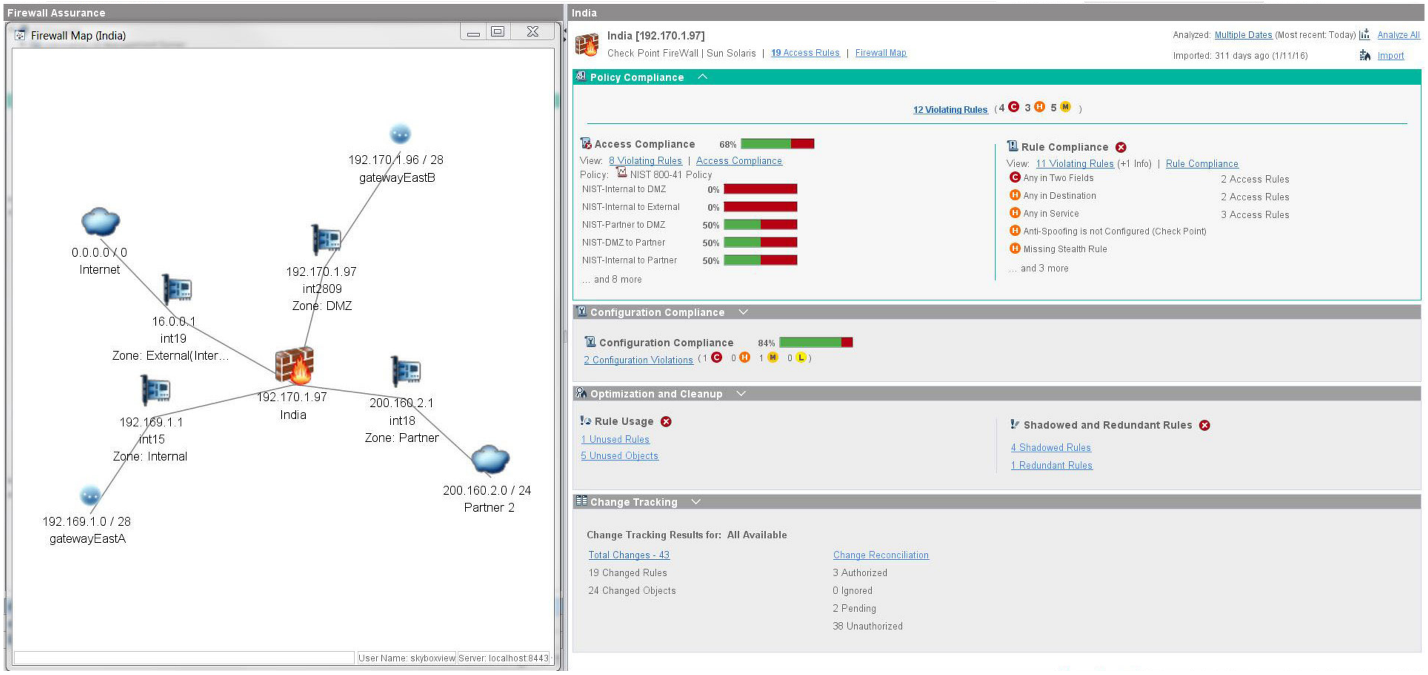
Many NCIIPC requirements revolve around auditing and documenting processes to ensure compliance. To meet such requirements, the first step is to enlist the various security teams in the organization to examine existing processes including those in firewall rule change management, networking device installation and configuration and new system and network identification. Skybox security policy management solutions provide the tools necessary to fulfill many of these tasks. With out–of–the–box reporting and compliance documentation as well as the ability to create your own customizable compliance reports, Skybox eases the resource burden that accompanies audits.

In addition to reporting capabilities, Skybox provides remediation plans to help focus IT resources, bring networks and processes into compliance with NCIIPC and other regulatory standards.

TECHNOLOGY

Skybox helps manage both network technology as well as the vulnerabilities existing on CII.

Understanding how connections are made and access is controlled across a network is fundamental to understanding an organization's unique attack surface. Firewalls are often the first line of defense for securing the network perimeter and CII, but configurations are difficult to manage and access policy implementation and changes are difficult to maintain. Skybox® Firewall Assurance provides robust firewall auditing capabilities, visualizing access paths and identifying redundant, shadowed or unused rule (see Figure 3).



India [192.170.1.97]
Check Point FireWall | Sun Solaris | 19 Access Rules | Firewall Map

Analyzed: Multiple Dates (Most recent: Today) Analyze All
Imported: 311 days ago (1/11/16) Import

Policy Compliance

12 Violating Rules (4 C 3 H 5 M)

Access Compliance 68%
View: 8 Violating Rules | Access Compliance
Policy: NIST 800-41 Policy

NIST-Internal to DMZ	0%
NIST-Internal to External	0%
NIST-Partner to DMZ	50%
NIST-DMZ to Partner	50%
NIST-Internal to Partner	50%

... and 8 more

Rule Compliance
View: 11 Violating Rules (+1 Info) | Rule Compliance

C Any in Two Fields	2 Access Rules
H Any in Destination	2 Access Rules
H Any in Service	3 Access Rules
H Anti-Spoofing is not Configured (Check Point)	
H Missing Stealth Rule	

... and 3 more

Configuration Compliance

Configuration Compliance 84%
2 Configuration Violations (1 C 0 H 1 M 0 L)

Optimization and Cleanup

Rule Usage
1 Unused Rules
5 Unused Objects

Shadowed and Redundant Rules
4 Shadowed Rules
1 Redundant Rules

Change Tracking

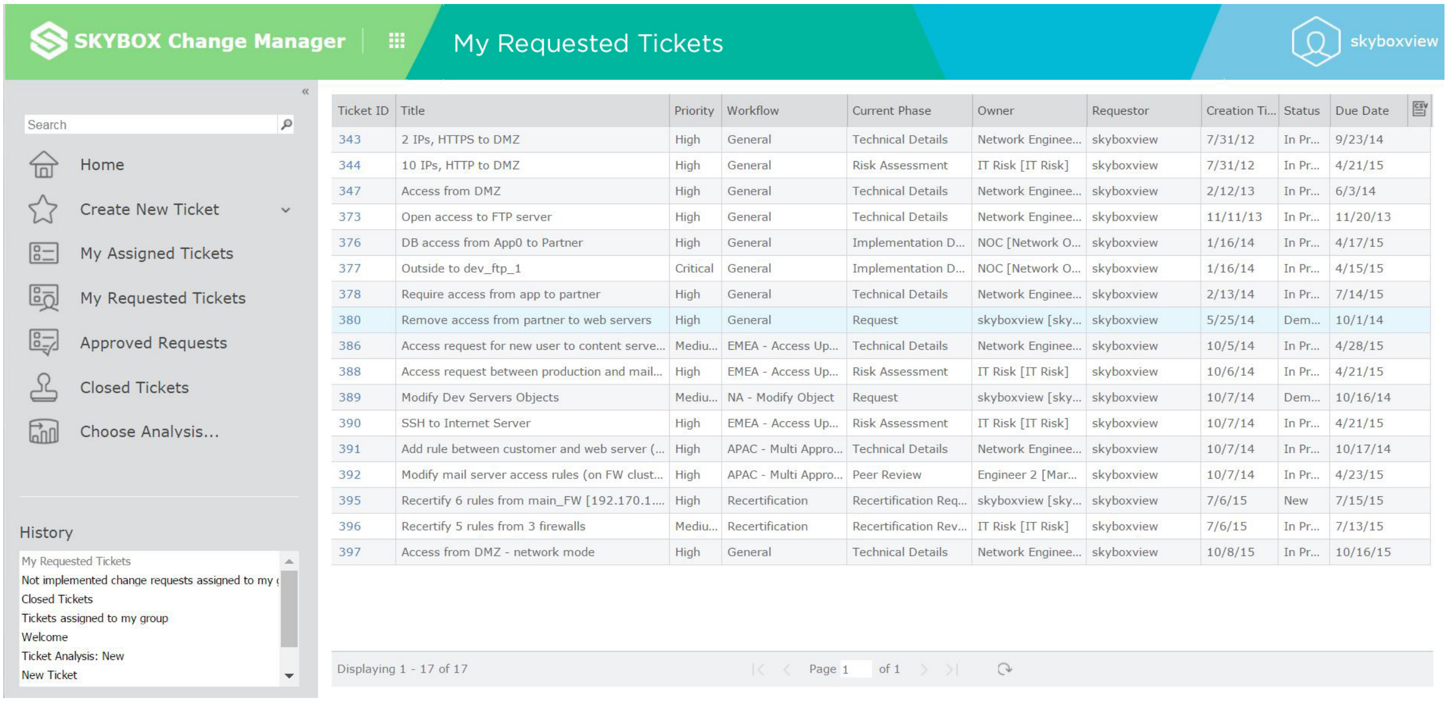
Change Tracking Results for: All Available

Total Changes - 43	Change Reconciliation
19 Changed Rules	3 Authorized
24 Changed Objects	0 Ignored
	2 Pending
	38 Unauthorized

FIGURE 3: Firewall Assurance network access map and analysis

In addition, Skybox® Change Manager provides a secure change management workflow that checks whether the rule or approval is necessary along with compliance and standards violations and rule recertification terms (see Figure 4).

But firewalls aren't the only factors to consider in terms of what is protecting or exposing CII. Unpatched or unmitigated vulnerabilities in endpoint and network devices give hackers the ability to run command line scripts that could elevate their access, allow the creation of backdoor accounts or identify and give access to additional network paths to data that is normally protected. With these elevated access controls, a hacker also has the ability to cover their tracks.



Ticket ID	Title	Priority	Workflow	Current Phase	Owner	Requestor	Creation Ti...	Status	Due Date
343	2 IPs, HTTPS to DMZ	High	General	Technical Details	Network Enginee...	skyboxview	7/31/12	In Pr...	9/23/14
344	10 IPs, HTTP to DMZ	High	General	Risk Assessment	IT Risk [IT Risk]	skyboxview	7/31/12	In Pr...	4/21/15
347	Access from DMZ	High	General	Technical Details	Network Enginee...	skyboxview	2/12/13	In Pr...	6/3/14
373	Open access to FTP server	High	General	Technical Details	Network Enginee...	skyboxview	11/11/13	In Pr...	11/20/13
376	DB access from App0 to Partner	High	General	Implementation D...	NOC [Network O...	skyboxview	1/16/14	In Pr...	4/17/15
377	Outside to dev_ftp_1	Critical	General	Implementation D...	NOC [Network O...	skyboxview	1/16/14	In Pr...	4/15/15
378	Require access from app to partner	High	General	Technical Details	Network Enginee...	skyboxview	2/13/14	In Pr...	7/14/15
380	Remove access from partner to web servers	High	General	Request	skyboxview [sky...	skyboxview	5/25/14	Dem...	10/1/14
386	Access request for new user to content serve...	Mediu...	EMEA - Access Up...	Technical Details	Network Enginee...	skyboxview	10/5/14	In Pr...	4/28/15
388	Access request between production and mail...	High	EMEA - Access Up...	Risk Assessment	IT Risk [IT Risk]	skyboxview	10/6/14	In Pr...	4/21/15
389	Modify Dev Servers Objects	Mediu...	NA - Modify Object	Request	skyboxview [sky...	skyboxview	10/7/14	Dem...	10/16/14
390	SSH to Internet Server	High	EMEA - Access Up...	Risk Assessment	IT Risk [IT Risk]	skyboxview	10/7/14	In Pr...	4/21/15
391	Add rule between customer and web server (...	High	APAC - Multi Appro...	Technical Details	Network Enginee...	skyboxview	10/7/14	In Pr...	10/17/14
392	Modify mail server access rules (on FW clust...	High	APAC - Multi Appro...	Peer Review	Engineer 2 [Mar...	skyboxview	10/7/14	In Pr...	4/23/15
395	Recertify 6 rules from main_FW [192.170.1....	High	Recertification	Recertification Req...	skyboxview [sky...	skyboxview	7/6/15	New	7/15/15
396	Recertify 5 rules from 3 firewalls	Mediu...	Recertification	Recertification Rev...	IT Risk [IT Risk]	skyboxview	7/6/15	In Pr...	7/13/15
397	Access from DMZ - network mode	High	General	Technical Details	Network Enginee...	skyboxview	10/8/15	In Pr...	10/16/15

Displaying 1 - 17 of 17   Page 1 of 1

FIGURE 4: Change Manager ticket assessment

Below are some of the NCIIPC requirements and how Skybox solutions can help align an organization's processes and technology to fulfill them:

NCIIP REQUIREMENT	SKYBOX TECHNOLOGIES
3: Information Security Department	• Conduct risk assessments, manage incidents and provide internal and external reporting • Ensure that all information systems within organization are adequately patched and updated
8: Limiting Administrator Privileges	• Limit access policies in perimeter protection devices to legitimate users only • Ensure default administrator accounts are disabled in all security hardware and software
9: Perimeter Protection	• Implement policies for the protection of the perimeter zone • Ensure use of firewalls with proper protection policies per the work requirement of the organization to block unwanted traffic • Align all critical changes to the security device infrastructure with formalized change management process
11: Risk Assessment Management	• Identify human threats and vulnerabilities that exist on the network • Perform quantitative and qualitative analysis that assigns risk levels based on confidentiality, integrity and availability • Analyze implications to the network, including asset impacted, severity and time duration • Support strategic prevention planning for potential exploits
28: Secure and Resilient Architecture Deployment	• Allow for the isolation of the DMZ from the internal network with the use of firewalls, IPSs and other security products including PKI, VPN and the hardening of remotely managed services • Regularly audit and pen test systems
30: Testing and Evaluation of Software and Hardware	• Ensure timely patching of software and hardware thus avoiding excessive time gaps • Recommend mitigations to reduce risk of exploit, if patches cannot be applied in a timely manner
31: Hardening of Software and Hardware	• Confirm device configurations are secure and passwords changed from the default setting • Ensure that unnecessary services, protocols and ports are closed or restricted and continuously monitored
35: APT Protection	• Configure protection devices to ensure access is limited to necessary users • Identify patches and malware protection updates so system software can be secured quickly • Ensure controls are in place to mitigate an exposure if necessary

TABLE 1: NCIIPC Requirements and Skybox

NCIIP REQUIREMENT	SKYBOX TECHNOLOGIES
36: Network Device Protection	• Confirm use of network devices and access control lists • Monitor paths of incoming and outgoing traffic • Track vulnerability remediation to ensure software is patched in a timely manner • Model network topology and architecture and identify segmentation improvements based on the sensitivity of data in certain areas
37: Cloud Protection	• Help ensure security of cloud-to-organization and cloud–to-cloud connections • Ensure barriers are erected to keep critical information separate and secure
40: Intranet Security	• Help isolate the intranet from the public internet through firewalls, proxies, routers and switches • Recommend patches and updates for all offline systems and security device software • Audit and pen test intranet networks to ensure attack vectors are closed

TABLE 1 (con't): NCIIPC Requirements and Skybox

Summary

A complete understanding of your attack surface is imperative to protecting the CII of both commercial and government organizations.

Gaining such an understanding requires a platform that models a network and analyzes data from multiple vendors and at multiple network levels. At a minimum, the platform must provide:

> A visual map of the attack surface, including network layers, firewall and network devices, IPSs, security management systems, assets, vulnerabilities and threats

> Insight into indicators of exposure (IOEs) that contribute to the attack surface; identify potential attack vectors and how they impact the organization as a whole

> Network topology visualization based on organizational structure, geographic sites, business units, gateways and network connections

Appendix

NCIIPC Guidelines and Controls for the Protection of Critical Information Infrastructure

CONTROL	AREA OF FOCUS
1	Identification of CII
2	Vertical and Horizontal Interdependencies
3	Information Security Department
4	Information Security Policy
5	Training and Skill Up-Gradation
6	Data Loss Prevention
7	Access Control Policies
8	Limiting Administrator Privileges
9	Perimeter Protection
10	Incident Response
11	Risk Assessment Management
12	Physical Security
13	Identification and Authentication
14	Maintenance Plans
15	Maintaining, Monitoring and Analyzing Logs
16	Penetration Testing
17	Data Storage, Hashing and Encryption
18	Feedback Mechanism for Threat Reporting to Government Agencies
19	Security Certifications
20	Asset and Inventory Management
21	Contingency Planning
22	Disaster Recovery Site
23	Predictable Failure Prevention
24	Information/Data Leakage Protection
25	DoS/DDoS Protection
26	Wi-Fi Security
27	Data Backup Plan
28	Secure Architecture Deployment
29	Web Application Security
30	Testing and Evaluation of Hardware and Software
31	Hardening of Hardware and Software
32	Periodic Audit and Vulnerability Assessment
33	Compliance of Security Recommendation
34	Checks and Balances for Negligence
35	APT Protection
36	Network Device Protection
37	Cloud Protection
38	Outsourcing and Vendor Security
39	Critical Information Disposal and Transfer
40	Intranet Security

TABLE 2: NCIIPC Guidelines and Controls for the Protection of Critical Information Infrastructure

About Skybox Security

Skybox arms security teams with a powerful set of security management solutions that extract insight from traditionally siloed data to give unprecedented visibility of the attack surface, including all indicators of exposure (IOEs). With Skybox, security leaders can quickly and accurately prioritize and address vulnerabilities and threat exposures in the context of their business environment and hybrid IT network.

www.skyboxsecurity.com | info@skyboxsecurity.com | +1 408 441 8060

Copyright © 2016 Skybox Security, Inc. All rights reserved. Skybox is a trademark of Skybox Security, Inc. All other registered or unregistered trademarks are the sole property of their respective owners. 11182016