National Institute of Standards and Technology
U.S. Department of Commerce

Developing a Framework to Improve Critical Infrastructure Cybersecurity
Request for Information
Docket No: 130208119-3119-01

COMMENTS OF ALCATEL-LUCENT

Alcatel-Lucent submits these Comments in response to the Request for Information ("RFI") of the National Institute of Standards and Technology ("NIST") on the developing a framework to improve critical infrastructure cybersecurity.

I. ALCATEL-LUCENT

Alcatel-Lucent is the trusted transformation partner of service providers, enterprises, and strategic industries, such as the energy and transportation industries, worldwide, providing solutions to deliver voice, data and video communications services to end-users. A leader in mobile, fixed, IP and optics technologies, and a pioneer in applications and services, Alcatel-Lucent was named on *MIT Technology Review*'s 2012 Top 50 list of the "World's Most Innovative Companies"[1] for breakthroughs such as its small cell, lightRadio™ technology, which cuts power consumption and operating costs on wireless networks while delivering lightning fast Internet access. Through such innovations, Alcatel-Lucent is making communications more sustainable, more affordable and more accessible. In achieving these goals, Alcatel-Lucent leverages the unrivaled technical and scientific expertise of Bell Labs, a leading innovator in the communications industry.

With operations across the globe and the most experienced global services organization in the industry, Alcatel-Lucent is a local partner with a global reach. Alcatel-

[1] *See* MIT Technology Review, 50 Disruptive Companies, available at http://www2.technologyreview.com/tr50/2012/, visited Jan. 21, 2013.

Lucent's presence in the United States, home to Bell Labs' global headquarters, is central to its position as a world leader in emerging telecommunications technologies.

Alcatel-Lucent recognizes security as a major concern and a critical part of each step in the deployment and operation of information and communications technology ("ICT") infrastructure and services. ICT security takes on even greater significance when it is related to critical infrastructure.

Alcatel-Lucent's security services ensure that solutions deployed by our customers are in line with best-in-class security standards and practices. We understand complex security requirements and issues inherent in next-generation networks and services, in particular as they apply to critical infrastructures and their operators.

The complexity of securing IP-based critical networks requires highly advanced skill sets. Alcatel-Lucent has this expertise across disciplines such as security assessments, planning, design and integration, within a well-established process that has been applied in very successful engagements with large enterprise, government, and service provider customers. The Alcatel-Lucent globally deployed security team offers comprehensive, multi-vendor, industry-leading reliability and security expertise that can guide the customer organization through the complexity of a transformation effort in a way that creates confidence and reduces risk. Managed security services has also become a vital part of the offering as more organizations recognize the importance of a professional force that can monitor network security and provide advanced security services on a 24 by 7 basis.

Alcatel-Lucent entered into a National Security Agreement ("NSA") with the U.S. Government at the time of its merger in 2006. This agreement requires Alcatel-Lucent to implement processes to protect the security and confidentiality of products or services provided to or affecting U.S. communications infrastructure or the U.S. Government worldwide.

II. RESPONSE TO RFI QUESTIONS

Alcatel-Lucent appreciates NIST's commitment to developing a cybersecurity framework that is "a living document that allows for ongoing consultation in order to address constantly evolving risks . . . ."[2] Alcatel-Lucent further agrees with NIST's approach when it states that, "the Cybersecurity Framework will not prescribe particular technological solutions or specifications,"[3] and that it, "will develop the Framework that is consistent with its mission to promote U.S. innovation and industrial competitiveness through the development of standards and guidelines in consultation with stakeholders in both government and industry."[4] Alcatel-Lucent applauds this approach and provides these comments to assist in the success of this "voluntary consensus-based process."[5]

Alcatel-Lucent looks forward to continued consultations as this process moves forward. Below, we address select questions set forth in the RFI, with a focus on the ICT sector and its interrelationship with other critical infrastructure sectors.

Current Risk Management Practices

1. What do organizations see as the greatest challenges in improving cybersecurity practices across critical infrastructure?

The greatest challenges to improving cybersecurity practices are the scope, complexity and rate of change of the problem. Responses to cybersecurity must be dynamic, making attempts to regulate in this area with static rules or technology mandates potentially counterproductive. It is for this reason that Alcatel-Lucent recommends an industry-led, standards based approach to cybersecurity.

---

[2] RFI at 9.

[3] *Id.* at 5.

[4] *Id.*

[5] *Id.* at 9.

Furthermore, each critical infrastructure sector operates independently of the others – there is no "one-size-fits-all" solution. Each sector has its own distinct business priorities, risk factors, cybersecurity concerns, primary regulatory agencies and regulations. These factors also have led to the lack of a common security lexicon to be used across critical infrastructure sectors. While there is no single cybersecurity solution that will work for every sector, a common security lexicon and a mapping of regulations between critical infrastructure sectors would be critical to any overarching cybersecurity framework.

2. What do organizations see as the greatest challenges in developing a cross-sector standards-based Framework for critical infrastructure?

Alcatel-Lucent sees four major challenges to developing a cross-sector, standards-based framework for critical infrastructure.

First, Alcatel-Lucent is concerned that any regulatory framework may be too prescriptive and, as a result, will limit the ability to rapidly respond to emerging threats. Such prescriptive standards will draw resources to mandatory requirements that would quickly become outmoded. Any framework must allow for and encourage adaptability and discretion based on sound risk management principles.

A second challenge arises from the unintended consequences that can result from a greater level of transparency of cybersecurity measures in the wake of a security breach. Companies want to do the right thing, but no system is perfect, especially in light of the pervasive, ever-evolving threats to various sectors. The increased visibility that comes with a standard framework and associated reporting of breaches can create commercial as well as operational risk for companies resulting in a natural resistance to adoption. The framework should thus focus on core principles

and evolving technologies to combat threats over the long haul, while providing sufficient flexibility and protection to combat the risks associated with transparency.

Third, as described above, each critical infrastructure sector operates independently with different regulatory frameworks and business conditions and is subject to different threats. A common lexicon as well as a harmonization of standards will be required to converge on a cross-sector security framework for critical infrastructure. A cross-sector security framework will also have to be flexible enough to adapt to the different business conditions and business priorities of critical infrastructure organizations. Common standards and protocols will also need to be developed to facilitate communication between the different critical infrastructure sectors.

Fourth, we increasingly live in a "borderless" business environment. Information and communication technologies are no longer confined to national boundaries. These technologies are truly global, inter-connected and inter-dependent, and thus require an international, coordinated and comprehensive legal framework to deal with cyber threats. It is therefore imperative that the framework developed in the U.S. incorporate international standards that can be adopted world-wide to best protect critical infrastructure systems.

3. Describe your organization's policies and procedures governing risk generally and cybersecurity risk specifically. How does senior management communicate and oversee these policies and procedures?

At Alcatel Lucent, risk management is addressed in its policy on risk management of physical assets and operations along with its insurance principles and risk engineering principles, both signed by the Chief Financial Officer. They cover the following areas: risk engineering, enterprise risk mapping (identification,

prioritization, and quantification), loss prevention and safety, and business continuity management. Alcatel-Lucent management oversees the overall Enterprise Risk Management ("ERM") process.

Alcatel-Lucent strives to incorporate appropriate security controls into information resources from the outset, governing risk generally and cybersecurity risk specifically. This is a key concept for any organization seeking to optimize security. Security protection measures and levels shall be commensurate with a resource's value to the corporation, as determined by the results of a formal risk assessment. Alcatel-Lucent has adopted detailed policies and procedures, including the following sample policies regarding information protection:

- Information resources shall have a designated information owner and resource administrator.
- Information owners shall have management responsibility for classifying and protecting their information resources into one of the following classifications: Open, Internal, Confidential, or Highly Confidential.
- Resource administrators shall protect their information resources according to the information classification level and guidance from Information Owner.
- Initial and periodic risk assessments shall be performed to determine the security controls required to protect information resources.
- Specific controls must be followed when handling, labeling, duplicating, distributing, storing, transporting and disposing of sensitive electronic or hard copy media.

At Alcatel-Lucent, communication of the cybersecurity and general security policies include mandatory training and awareness messages. Further education as well as oversight are implemented through a program of policy deployment, compliance self assessments supported by reviews of responses and evidence by security subject matter experts, enforcement of outsourcing contractual obligations, and security reviews in activities that have the potential to introduce risk (e.g.

projects, third party connections, etc.). A similar approach is recommended for other organizations seeking to optimize security practices.

4. Where do organizations locate their cybersecurity risk management program/office?

Organizations often locate their information Security function under the office of the Chief Information Security Officer, as does Alcatel-Lucent. However, cybersecurity risk management responsibilities should also be embedded within several offices within a company, including, for example, Information Security, Information Technology Operations, Legal, Chief Technology Officer and Chief Security Officer/Physical Security.

5. How do organizations define and assess risk generally and cybersecurity risk specifically?

A risk management process should be a core element of any organization's risk management framework. Alcatel-Lucent defines and assesses risks through a number of processes. Alcatel-Lucent utilizes an overall ERM process for identification and management of key business risks. The ERM process is overseen by the Management Committee and the Audit & Finance Committee. It is based on an 80-line standard risk register (discussed further below in response to question 7), and risks are assessed in terms of severity of the impact, likelihood of occurrence and control effectiveness. Risks having monetary exposures are quantified. Each key risk has its mitigating action plans identified and monitored. Cybersecurity risks are included in the risk catalogue.

As part of our overall risk management framework, there is an underlying risk assessment process that is conducted across all operating units on an annual basis

focused on information security risks. An overall information security risk mitigation plan is developed and executed at both the program and operating unit level. A key component for each operating unit is the requirement to identify and conduct a formal assessment of critical ecosystems. This includes the evaluation of threats, risks and business impacts, with particular focus on ecosystems most likely to be targets of advanced persistent threat ("APT") attacks. Assessment elements also include perimeter definition, identification of applicable solutions/controls and compliance assessments of the associated assets and environments.

6. To what extent is cybersecurity risk incorporated into organizations' overarching enterprise risk management?

Alcatel-Lucent identifies key cybersecurity risks through the information security compliance program included in the ERM process and risk register. (See response to question 5, above). Incorporating cybersecurity into this overall risk management process is critical to placing cybersecurity risks into a proper business and operational risk context. In this way, internal cybersecurity policies also leverage and build upon existing processes and practices, which is an important concept for the cybersecurity framework.

7. What standards, guidelines, best practices, and tools are organizations using to understand, measure, and manage risk at the management, operational, and technical levels?

Alcatel-Lucent's ERM process has been in place for more than a decade. Our ERM process complies with the integrated Committee of Sponsoring Organizations of the Treadway Commission ("COSO") II framework (which allows companies to structure all kinds of risks and organize appropriate mitigating actions), and aligns with the recommendations of the French Autorité des Marchés Financiers and the

Sarbanes-Oxley Act. This risk framework covers 80 lines of risk in the areas of operations, finance, strategy, HR, security, and legal and compliance. The ERM workflow is supported by an integrated risk management platform.

Alcatel-Lucent recommends the following framework to understand cybersecurity risk. Alcatel-Lucent's overall risk management framework is built using a commercially available governance, risk and compliance ("GRC") platform. Our risk management approach leverages best practice approaches incorporated into the policy management, asset management and risk management solutions that are included in this platform, with customizations that cover ISO compliance, Critical Ecosystems, Third Party Security Management and Project Assessments. Alcatel-Lucent's own processes and practices incorporate concepts from ISO (27005), ISF Cyber resilience framework and CMM, and NIST (SP800-53r4, SP800-30, SP800-37, SP800-137, SP800-39) and include:

- system/environment classification based on detailed data element inventory and associated criticality classification;
- risk management & compliance reviews incorporated into the system development lifecycle;
- ongoing compliance management based on system criticality, collection of risks into a common risk register; and
- formalized risk evaluation and acceptance, action plans/tracking to remediate risks, and roll up into the enterprise risk management process.

For technical risk management (i.e. management of risks associated with product development and network deployment), enterprises should consider multiple standards and customize them to address business priorities. Alcatel-Lucent's internal risk and threat management standards were constructed with reference to external standards, practices and guidelines augmented with R&D expertise and insights. The external collateral referenced by Alcatel-Lucent's internal standards includes:

- ETSI TS 102 165-1 V4.2.1 (2006-12) TISPAN; Methods and protocols; Part 1: Method and pro forma for Threat, Risk, Vulnerability Analysis;
- NIST SP 800-30rev1 Guide for Conducting Risk Assessments; and
- ISO/IEC 27005: Information Technology – Security Techniques – Information Security Risk Management.

9. What organizational critical assets are interdependent upon other critical physical and information infrastructures, including telecommunications, energy, financial services, water, and transportation sectors?

As an initial step to dealing with an organization's dependence on other critical physical and information infrastructures, organizations must identify their own critical assets using techniques such as (i) a risk-based analysis; or (ii) "bright-line" criteria. A risk-based analysis evaluates the criticality of a given asset to an organization based on factors such as its exposure to attack vectors and the impact to the organization of a successful cyber attack on the asset. Bright-line criteria are more deterministic in that an asset is evaluated against a predefined list of criteria constituting a critical asset. If the asset satisfies one or more of the criteria, it is classified as a critical asset.

Once an organization identifies its critical assets, each critical asset's dependencies on various critical infrastructures should be evaluated and controls put in place to provide continuity of operations in the event that the service provided by a critical infrastructure is interrupted. Examples of "controls" would be battery backup in case electrical power is interrupted; multiple telecommunications carriers and access diversity in case a primary telecommunications service is disrupted; and geographical redundancy in case an event impacts an entire locality.

10. What performance goals do organizations adopt to ensure their ability to provide essential services while managing cybersecurity risk?

The concept of critical ecosystem identification and protection should be a core element of the cybersecurity framework.

Alcatel-Lucent conducts business continuity and disaster recovery planning, including the classification of our systems into categories that indicate the level of criticality of each system (e.g. platinum, gold, silver or bronze). This serves as a foundational practice. Cybersecurity risk is incorporated into our assessments of critical ecosystems. In these assessments, all aspects of the ecosystem (internal and external) are identified and assessed. Remediation action plans are developed to ensure that effective controls to mitigate the risks to these environments have been implemented. We establish goals for the identification, classification, assessment and remediation of these critical information ecosystems to ensure that the cybersecurity risks to the most critical assets are identified and mitigated. Progress on critical information protection assessments, gaps and remediation plans are tracked.

12. What role(s) do or should national/international standards and organizations that develop national/international standards play in critical infrastructure cybersecurity conformity assessment?

Standards are commonly used as inputs or references by critical infrastructure operators to define their expectations in terms of security controls to be deployed within their infrastructures. Such standards are therefore used as baselines to assess conformity of solutions sold by vendors to such operators. Throughout this document, Alcatel-Lucent references the multiple standards and best practices that guide organizations in securing their infrastructure.

Use of Frameworks, Standards, Guidelines, and Best Practices

1. ***What additional approaches already exist?***

A wide range of standards, guidelines and best practices already exist that can be (and, indeed, are) applied to protection of information and information systems in critical infrastructure. The following are examples of significant domain-agnostic and sector-specific assets:

- Domain-agnostic:
    - ISO/IEC Standards (including 27000 family, 1335, 15408)
    - NIST (including 800-30, 800-53, 800-37, 800-39)
    - SANS 20 Critical Controls: Consensus Audit Guidelines
    - COBIT Security Baseline
    - Information Security Forum Standard of Good Practice, Cyber Resilience Framework and CMM
    - Shared Assessment model/SIG
    - Network Reliability and Interoperability Council ("NRIC")/Communications Security, Reliability and Interoperability Council ("CSRIC") industry best practices ("NRIC/CSRIC Best Practices"), available at http://www.atis.org/bestpractices/Search.aspx.
- Domain, technology or sector-specific:
    - NERC CIP (power domain)
    - NIST 800-82 (industrial control systems)
    - NISTIR 7628 (smart grid)
    - 3GPP TS.33.102, TS.35.20x (wireless telecommunications)

Additionally, there are many domain-specific standards bodies and industry fora. ATIS is one example in the telecommunications domain.

2. ***Which of these approaches apply across sectors?***

The domain-agnostic examples in the previous response can apply across sectors. Technology-specific standards also can be applied across sectors that employ similar technology – for example, NIST 800-82 can be relevant to the use of SCADA in multiple sectors, including energy, water and transport. Standards involving information security, privacy and physical security are also applicable across critical infrastructure sectors.

Additionally, existing sector-specific standards, practices or guidelines could be adapted for use in related sectors. An example could be the possible construction of a standard for critical infrastructure domains such as gas or transport based on or informed by the assets already established for the power domain.

4. ***What, if any, are the limitations of using such approaches?***

One barrier to the adoption of standards, best practices and guidelines is the fact that there are multiple potential sources for those standards, best practices and guidelines to consider. The various sources can overlap and could potentially be inconsistent in some areas. Thus, for the purpose of an overarching cybersecurity framework, it would be desirable to develop a single cybersecurity lexicon to help bridge those many sources. Even assuming a common set of standards as a reference, however, often it is necessary or desirable to customize the original asset to the particular business needs of the organization.

Another limitation is the fact that many of the potential sources were published some time ago, before significant developments such as widespread virtualization, outsourcing, hosting and cloud-based deployments. The time taken for standards to adapt, or for new standards to be published, can be significant. Industry

"best practices," such as those developed through industry participants at NRIC/CSRIC provide a much quicker vehicle for conveying up-to-date processes and procedures. Because they are not intended to be mandatory, technical experts can convene quickly and openly and identify the best practice that applies to changing technologies and configurations.

A potential limitation of standards-based approaches to information security can potentially be an excessive focus on complying with that standard at the cost of genuine focus on informed and proactive risk management practices applicable to a particular organization at a particular time. It is important to guard against standards-based approaches creating a false sense of security or even impeding agility in security management.

As discussed previously, different critical infrastructure sectors have different business imperatives, different levels of technological sophistication, and a differing ability to implement compensating controls. For example, critical infrastructure sectors employing SCADA systems heavily rely on physical security and logical separation of networks to protect their critical systems. Other critical infrastructures that require direct interfaces to the Internet do not have that luxury. These types of differences almost by definition require distinct approaches to cybersecurity.

5. ***What, if any, modifications could make these approaches more useful?***

Approaches based on applying existing standards can be made more useful through guidelines provided by the relevant standards body on how to apply key assets in particular domains, based on consensus, voluntary compliance, and best practices. Again, adoption of a common lexicon across critical infrastructure can also aid in making standards-based approaches more useful and effective.

Another way to improve the results of standards-based approaches is to ensure that the standards evolve as technologies and the threat landscape evolves. The applicable standards body should ensure that the standards remains current, for example, through a periodic gap-analysis of existing standards to identify areas where new or amended standards are required.

6. ***How do these approaches take into account sector-specific needs?***

These approaches need to be flexible enough to address the varying business priorities, varying threats to and different technologies used by the different critical infrastructure sectors. Technology agnostic standards coupled with sector-specific standards provide this flexibility provided they are kept up to date to reflect the changing threat environment.

9. ***What other outreach efforts would be helpful?***

The following activities would be helpful in creating a cross-sector security framework:

- Define a standard security lexicon of general security principles for critical infrastructure sectors.
- Sector-specific training on general security principles in the sector's terminology. Awareness of supply chain security requirements.
- Security framework that harmonizes sector-specific security standards, guidelines and regulations to standard security lexicon.
- Institute and maintain a catalog of threats for use by critical infrastructure sectors.
- Convene a forum that facilitates communication among critical infrastructure sectors without concern of disclosure by the forum of business-sensitive information.

Specific Industry Practices

1. Are these practices widely used throughout critical infrastructure and industry?

The RFI lists a number of "core practices" used by critical infrastructure, described in further detail below. Certain critical infrastructure sectors may present different risk factors leading to different emphases, but all of the core practices are accounted for to some degree. For example, energy sector places greater emphasis on core practices promoting high availability and reliability; the banking and finance sector emphasizes core practices promoting data integrity; and the health care and public health sector emphasizes core practices promoting privacy.

Separation of business from operational systems is typically implemented by perimeter networks (sometimes referred to as "DMZs") that prevent direct access to the critical infrastructure operational systems (e.g., SCADA systems) by entities outside of the operational zone. These could be entities within the business or entities external to the business.

Encryption and key management are used by organizations to protect the privacy and confidentiality of data at rest and in-transit. Cryptographic algorithms use keys to manage the data encryption and decryption process. Key management is the process used to distribute the keys to the appropriate individuals.

Identification and authorization of users accessing systems is required to ensure only authorized individuals can access systems. Each individual user should have their own unique user ID so that their actions on the system can be accurately tracked, thus ensuring user accountability. Two factor authentication (e.g., user ID and password, plus secure token) should be used on critical systems to protect user passwords from being compromised. Role-based access control ("RBAC") based on

the principal of least privilege should also be used to ensure users are not able to access unnecessary system capabilities or information.

Asset identification and management informs organizations about what they need to protect. Obviously, it is important to keep an organization's asset list up to date; asset management is responsible for maintaining the asset list. There are multiple automated tools available for identifying networked assets. Maintaining the assets themselves is another aspect of asset management. For example, patch management can be considered a subset of asset management.

Monitoring and incident detection tools and capabilities provide situational awareness about an organization's network and operations. In addition to traditional firewall and Intrusion Detection Systems/Intrusion Protection Systems ("IDS/IPS") and next generation Security Information and Event Management ("SIEM") systems combined with analytic software can provide a rapid indication of the presence of an attacker or APT on an organization's network, in an organization's system, or exfiltrating an organization's information.

Incident handling policies and procedures must be documented, reviewed, and exercised on a periodic basis. An incident handling policy provides guidance regarding notification and handling of security incidents in a structured and consistent manner. Incident handling procedures describe what is to be done and who is to do it when an incident occurs. It is important that the policy be reviewed and exercised on a periodic basis because the threat environment is constantly changing and organizational dynamics are subject to change as well.

Mission/system resiliency practices are intended to provide continuity of operations to an organization's primary business. Typical technical resiliency

practices focus on redundancy: redundant energy supplies, redundant operations centers, redundant data centers, redundant telecommunications links, etc.

Security engineering practices should be followed that design security into an organization's systems from their start through their end of life. An organization should have a methodology in place that includes planning for security during project inception, implementing and testing for security during project development, secure deployment during project rollout, maintaining security during the project's operational life, and secure decommissioning at the project's end of life.

2. ***How do these practices relate to existing international standards and practices?***

The following are examples of existing standards and practices that relate to the specific practices described above:

• Separation of business from operational systems

NIST 800-80

NRIC/CSRIC Best Practice 8-6-5170

• Use of encryption and key management;

NIST 800-53 (IA-7, SC-12, SC-13, SC-17)

ISO/IEC 27001 (A12.3.1, A12.3.2, A15.1.6, A15.2.2)

NRIC/CSRIC Best Practice 8-6-8028

• Identification and authorization of users accessing systems

NIST 800-53 (AC-1..22, IA-1.8)

ISO/IEC 27001 (A11.*)

NERC (CIP-003, CIP-005)

NRIC/CSRIC Best Practice 8-7-8083; 8-7-8086

SANS 20 (CC-8, CC-9, CC-11)

Vulnerability management (CERT, ICS-CERT)

• Asset identification and management

ISO/IEC 27001 (A7.1.1.3, A8.3.2, A9.2.4.6, A10.7.1.2)

NIST 800-53 (CM-8, PM-5)

SANS 20 (CC-1, CC-2)

NERC (CIP-002, CIP-003)

NRIC/CSRIC Best Practices 8-7-8089, 8-7-0510.

• Monitoring and incident detection tools and capabilities

NIST SP 800-61: Computer Security Incident Handling Guide

ISO/IEC 27035: Information Technology – Security Techniques –Information Security Incident Management

ICS CERT: Recommended Practice: Developing an Industrial Control Systems Cybersecurity Incident Response Capability.

NRIC/CSRIC Best Practice 8-8-8072

• Incident handling policies and procedures

ISO/IEC 27001 (A13.1.1..2, A.13.2.1.3)

NIST 800-53 (IR-1.11)

SANS 20 (CC-18)

NERC (CIP-008)

NRIC/CSRIC Best Practices 8-7-1008, 8-7-5092, 8-7-8062, 8-8-8061

• Mission/system resiliency practices

NIST SP 800-34: Contingency Planning Guide for Federal Information Systems

NERC: Security Guideline for the Electricity Sector: Continuity of Business Processes and Operations Operational Functions

NRIC/CSRIC Best Practices 8-7-1048, 8-7-5204, 8-7-5222, 8-7-5223

• Security engineering practices

NIST SP 800-27: Engineering Principles for Information Technology Security

ISO/IEC 21827: Security Techniques – Systems Security Engineering – Capability Maturity Model ®

NRIC/CSRIC Best Practices 8-7-0565, 8-7-5167, 8-7-5218, 8-8-8033

3. ***Which of these practices do commenters see as being the most critical for the secure operation of critical infrastructure?***

Alcatel-Lucent believes that a defense-in-depth practice is the most critical practice for the secure operation of critical infrastructure followed by adherence to a security lifecycle. Defense-in-depth consists of placing multiple layers of security controls throughout a cyber system in order to use multiple defense mechanisms to defend the system against attack. These security controls should be in place throughout the system's lifecycle and can include the personnel, procedural, technical and physical controls listed above. A defense-in-depth practice can not only prevent security breaches, it can also delay an attacker's ability to accomplish their objective, thus giving an organization more time to detect and respond to the security breach. Finally, a defense-in-depth practice also includes practices designed to keep the system up and running in the face of an attack.

A security lifecycle consists of security engineering practices that are performed at every stage of the system lifecycle; from system conceptualization through decommissioning. A security lifecycle includes planning for security during project inception, implementing and testing for security during project development, secure deployment during project rollout, maintaining security during the project's operational life, and secure decommissioning at the project's end of life.

5. ***Which of these practices pose the most significant implementation challenge****?*

Although implementing technical practices such as encryption and key management, access control and authentication, and incident detection may be technically challenging, those practices that span multiple organizations, or require organizational change pose the most significant implementation challenge.

Organizations that historically have not been involved in security are resistant to taking on additional responsibility without being convinced. In addition, for organizations that consist of business divisions that operate independently, such organizations may not be amenable to implementing a practice spanning horizontally across all organizations of a company.

Implementing a security engineering practice consisting of security activities performed throughout a system's lifecycle requires implementation of security practices by design, engineering, operations and maintenance teams. Each of these teams needs to see the value of the security activities they are being asked to perform and agree to perform them. The education and negotiation required to implement a security engineering practice can be very challenging and time consuming.

Redesigning business processes and networks in order to separate business from operational systems can also be very challenging for exactly the opposite reason. Now organizations are being asked to do without access to information and systems they have grown accustomed to using. Challenging and time consuming education and negotiations are required to implement this practice as well.

6. ***How are standards or guidelines utilized by organizations in the implementation of these practices?***

Alcatel-Lucent takes a proactive approach to defining and implementing standards and guidelines in our products. We actively contribute our communications

and security expertise to numerous standards bodies. Alcatel-Lucent representatives on standards bodies work closely with Alcatel-Lucent-internal organizations responsible for developing our products. This relationship ensures that Alcatel-Lucent products implement the latest security capabilities as quickly as possible. A product's compliance to a given security standard will be placed in the product roadmap for earliest possible inclusion in the product.

7. Do organizations have a methodology in place for the proper allocation of business resources to invest in, create, and maintain IT standards?

Organizations allocate resources based on business risk. Alcatel-Lucent takes a proactive approach to participation in standards bodies. This approach allows us to keep abreast of emerging standards and develop plans for their implementation. These plans incorporate performing a business risk assessment and allocating the appropriate resources at the appropriate time based on the result of the assessment.

Alcatel-Lucent takes a surgical approach in determining in which standards bodies to participate and to which standards we contribute. There are so many standards bodies that this is the only approach that makes business sense. An evaluation is made involving the effectiveness of the standards body, its influence on the telecommunications industry, and its impact on Alcatel-Lucent product lines before deciding to participate in a given standards body or on a given standard.

8. Do organizations have a formal escalation process to address cybersecurity risks that suddenly increase in severity?

It is standard practice to have a formal incident escalation and crisis management process that is used for information security and cybersecurity incidents.

10. ***What are the international implications of this Framework on your global business or in policymaking in other countries?***

NIST should take care to minimize the international implications of this framework on global business by incorporating international standards that can be applied across borders. If the framework trends toward U.S. specific standards, it could lead to industry having to cater to multiple different (but not necessarily more or less secure) country requirements. International harmonization and use of existing international standards is of paramount importance to increasing security without harming the U.S. economy or innovation.

* * * * *

Respectfully submitted,

Alcatel-Lucent

/s/
Kevin Krufky, Vice President
Jeffrey Marks, Sr. Counsel – Director Regulatory Affairs

Public Affairs, Americas Region
1100 New York, Avenue, N.W.
Suite 640 West Tower
Washington, D.C. 20005

April 8, 2013