"Developing a Framework to Improve Critical Infrastructure Cybersecurity"
Submission from Huawei Technologies[i]
Response to RFI - Docket Number 130208119–3119–01

Current Risk Management Practices

NIST solicits information about how organizations assess risk; how cybersecurity factors into that risk assessment; the current usage of existing cybersecurity frameworks, standards, and guidelines; and other management practices related to cybersecurity. In addition, NIST is interested in understanding whether particular frameworks, standards, guidelines, and/or best practices are mandated by legal or regulatory requirements and the challenges organizations perceive in meeting such requirements. This will assist in NIST's goal of developing a Framework that includes and identifies common practices across sectors.

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

As the NIST RFI highlights, critical infrastructures range from telecommunications to energy, financial services, water supply, transportation, and beyond. Common and global standards and disciplines vary in terms of detail and maturity across these various sectors, in some cases overlapping, in others conflicting, in yet others creating redundancies. From the perspective of the information communications technology (ICT) industry, Huawei believes that perhaps the greatest challenge remains the establishment of consistent, effective and universal – industry-wide – security assurance standards and disciplines. There are a myriad of different bodies and initiatives focused on achieving such standards. Focus and order will be required if we are to realize our common industry goal. Ultimately, Huawei believes that the public-private establishment of baseline security assurance standards for the ICT industry should cover all key components of the end-to-end lifecycle of ICT products, including R&D, product development, procurement, supply chain, pre-installation product evaluation, and trusted delivery/installation, and post-installation updates and servicing. Such a comprehensive approach, informed by risk, is critical to an effective approach to addressing cybersecurity challenges.

Huawei hopes that this approach can be followed internationally to facilitate coordination of efforts regarding principles of privacy, data protection, and cyber security. Given the global nature of the ICT supply chain, it is very important for vendors, service providers, and corporations to have consistent standards and approaches as they conduct business across multiple continents and various countries.

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

No comment.

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?

1) General risk

Based on the Committee of Sponsoring Organizations of the Treadway Commission (COSO) framework and in line with our organizational structure and operating model, Huawei designed and implemented an enterprise risk management (ERM) system with a corresponding ERM policy. Huawei also established the ERM Department and an operational mechanism. The company ensures the continuity of our business operations by taking risks into account when making strategic decisions and planning, while also preemptively controlling risks in our business plans and execution.

Strategic Risks

Intense competition: The markets Huawei operates in are intensely competitive in terms of price, functionality, and service quality as well as the timing of new product and service development. In certain geographical markets, our main competitors may offer more attractive prices, products, services, or other incentives. The rapid development of science and technology, and changes in alternative technologies or industry standards, will lead to shorter product lifecycles and may also increase the number of entrants into the markets in which we operate.

In this market context, the ability to fully understand and satisfy customer needs is a prerequisite as technologies change rapidly and competition intensifies. To stay competitive and protect our operating results, we must constantly introduce new products and functionalities into the market while reducing the cost of new and existing products.

External Risks

- Economic environment: The global economic downturn could cause telecom carriers to postpone investments or initiate other cost-cutting measures to improve their financial position. These factors could result in reduced demand for network infrastructure and services, which would in turn affect Huawei's operating results.
- Country-specific risks: Huawei conducts business in more than 140 countries. Operating in these counties involves certain risks, such as civil unrest, economic and political instability, trade protection, imposition of exchange controls, nationalization of private assets, and debts. All these risks require Huawei to have a high aptitude for risk management. In addition, there may be uncertainties in the legal environment in certain regions. Although we strive to comply with all such laws and regulations, unintentional violations could have material adverse effects on our business.
- Natural disasters: Earthquakes, floods, and other natural disasters may slow down or even prevent delivery and impact the company's supply chain operations.

Operational Risks

- Business continuity: Although Huawei strives to avoid single-source supplier solutions, it is not always possible. To find an alternative supplier or to re-design products may take significant time. As such, supply and delivery of our products to our customers could be disrupted if any of our single-source suppliers were to meet with difficulties. To mitigate this risk, we periodically evaluate and conduct audits on our suppliers, and initiate product replacements or redesign to reduce the risk of obsolescence.

- Rising labor costs: Increasing labor costs in China may offset the company's efforts to reduce our product cost and ultimately affect our profitability.
- Information security: While Huawei has judiciously adopted information security measures to protect our intellectual property rights, they may not be adequate to prevent infringement or improper use of our information, patents, or licensing. Misappropriations of this nature will cause losses to Huawei even though we may be protected to some extent by intellectual property law.

Financial Risks

Include liquidity risk, currency risk, interest rate risk, credit risk, sales financing, etc.

Huawei further improved its financial risk management policies and processes to enhance the company's ability to withstand financial risks and better strategize to achieve business development goals.

2) Cybersecurity risk

As a global leading provider of information and communications solutions, we are engaged in providing information network products and service to society. The global network needs to be stable at all times. It is our primary social responsibility to support the assurance of a stable and secure network for customers, including in times of natural disasters such as earthquake and tsunami, and other emergencies like war.We understand the sensitivity of the ICT industry and the vulnerability of advanced technology. The end-to-end cyber security assurance system has been established and implemented in terms of policy, organization, process, management, technology and specifications. Huawei started its cyber security journey in 1999 when it published its first set of security technical regulations to enhance the security of products and solutions. In 2011, our founder and CEO, Ren Zhengfei, fully endorsed the strategy and issued the following Cyber Security Assurance policy that further reinforced and enhanced our commitment:

“As a global leading telecom solutions provider, Huawei is fully aware of the importance of cyber security and understands the concerns of various governments and customers about security. With the constant evolution and development of the telecom industry and information technology, security threats and challenges are increasing, which intensify our concerns about cyber security. Huawei will therefore pay a great deal more attention to this issue and has long been dedicated to adopting feasible and effective measures to improve the security of its products and services, thus helping customers to reduce and avoid security risks and building trust and confidence in Huawei’s business. Huawei believes that the establishment of an open, transparent and visible security assurance framework will be conducive to the sound and sustainable development of industry chains and technological innovation; it will also facilitate smooth and secure communications among people.

In light of the foregoing, Huawei hereby undertakes that as a crucial company strategy, based on compliance with the applicable laws, regulations, standards of relevant countries and regions, and by reference to the industry best practice, it has established and will constantly optimize an end-to-end cyber security assurance system. Such a system will incorporate aspects from corporate policies, organizational structure, business processes, technology and standard practice. Huawei has been actively tackling the challenges of cyber security through partnerships with governments, customers, and partners in an open and transparent manner. In addition, Huawei guarantees that its commitment to cyber security will never be outweighed by the consideration of commercial interests.

From an organizational perspective, the Global Cyber Security Committee (GCSC), as the top-level cyber security management body of Huawei, is responsible for ratifying the strategy of cyber security assurance. The Global Cyber Security Officer (GCSO) is a significantly important member of GCSC, in charge of developing this strategy and managing and supervising its implementation. The system will be adopted globally by all departments within Huawei to ensure consistency of implementation. The GCSO shall also endeavour to facilitate effective communication between Huawei and all stakeholders, including governments, customers, partners and employees. The GCSO reports directly to the CEO of Huawei.

In terms of business processes, security assurance shall be integrated into all business processes relating to R&D, the supply chain, sales and marketing, delivery, and technical services. Such integration, as the fundamental requirement of the quality management system, will be implemented under the guidance of management regulations and technical specifications. In addition, Huawei will reinforce the implementation of the cyber security assurance system by conducting internal auditing and receiving external certification and auditing from security authorities or independent third-party agencies. Furthermore, Huawei has already been certified to BS7799-2/ISO27001 accreditation since 2004.

In connection with personnel management, our employees, partners and consultants are required to comply with cyber security policies and requirements made by Huawei and receive appropriate training so that the concept of security is deeply rooted throughout Huawei. To promote cyber security, Huawei will reward employees who take an active part in cyber security assurance and will take appropriate action against those who violate cyber assurance policies. Employees may also incur personal legal liability for violation of relevant laws and regulations.

Taking on an open, transparent and sincere attitude, Huawei is willing to work with all governments, customers and partners through various channels to jointly cope with cyber security threats and challenges from cyber security. Huawei will set up regional security certification centers if necessary. These certification centers will be made highly transparent to local governments and customers, and Huawei will allow its products to be inspected by people authorized by local governments to ensure the security of Huawei's products and delivery service. Meanwhile, Huawei has been proactively involved in the telecom cyber security standardization activities led by ITU-T, 3GPP, and IETF etc., and has joined security organizations such as FIRST and partnered with mainstream security companies to ensure the cyber security of its customers and promote the healthy development of industries."

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

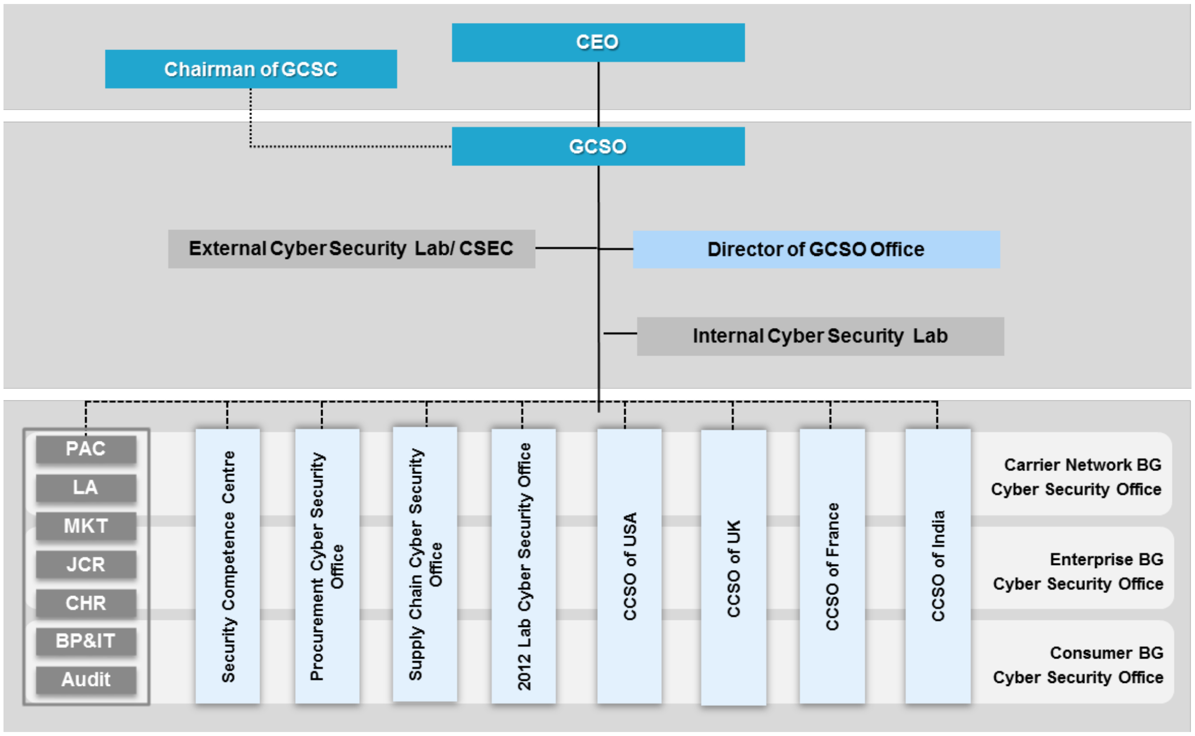
From an organizational perspective, the Global Cyber Security Committee (GCSC), as the top-level cyber security management body of Huawei, is responsible for ratifying the strategy of cyber security assurance. The Global Cyber Security Officer (GCSO) is a significantly important member of GCSC, in charge of developing this strategy and managing and supervising its implementation. The system will be adopted globally by all departments within Huawei to ensure consistency of implementation. The GCSO shall also endeavour to facilitate effective communication between

Huawei and all stakeholders, including governments, customers, partners and employees. The GCSO reports directly to the CEO of Huawei.

GCSO: Leading the team to develop the security strategy, establishing the cyber security assurance system internally, supporting GR/PR and supporting global accounts customers externally.

GCSO Office: coordinating related departments to formulate detailed operational rules and actions to support the strategy and its implementation, promoting the application, auditing and tracking of the implementation. The company focal point to identify and resolve cyber security issues

Regional/ Department Security Officers: Accountable for working with GCSO to identify changes to departmental/ business unit processes so that the cyber security strategy and its requirements are fully imbedded in their areas. They are also experts in their own right and contribute to the development and enhancement of the strategy.


CEO
Chairman of GCSC
GCSO
External Cyber Security Lab/ CSEC
Director of GCSO Office
Internal Cyber Security Lab
PAC
LA
MKT
JCR
CHR
BP&IT
Audit
Security Competence Centre
Procurement Cyber Security Office
Supply Chain Cyber Security Office
2012 Lab Cyber Security Office
CCSO of USA
CCSO of UK
CCSO of France
CCSO of India
Carrier Network BG Cyber Security Office
Enterprise BG Cyber Security Office
Consumer BG Cyber Security Office

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

1） For the definition and evaluation of general risk, please refer to the answers to Question 3.
2） For cyber security risk

Cyber security is to ensure the availability, integrity, confidentiality, traceability, and robustness of products, solutions, and services based on a legal framework. Additionally, it protects the customers' or users' communication content, personal data and privacy carried therein, and the flow of unbiased information.

Global technology companies have to protect their technology from a range of malicious uses; these include:

Use in sabotage: Control, paralysis, interruption or take-down of networks or infrastructures

Use in espionage: Enabling a third-party to illegally spy on another person or entity through their technology

Becoming the extension of another group/state: The Company's global reach and capability being directed by another government/group to act against another state/sub-state, group or individual

Lack of precaution and competence: Lack of best practice, end-to-end cyber security capability renders the technology an easy attack vector – used by any of the threat actors to use the company's technology or capability for an illegal or inappropriate purpose

All companies that develop and support technology must build in risk-informed mechanisms, counter-measures, policies and procedures that limit the likelihood of perceived or actual threats from being successful. These include, but are not limited to:

- Hardware/software "kill switch" (fixed or remotely controlled)
- Control via backdoors, Trojans, viruses and software logic bombs
- The company (individuals or groups) is instructed to close down networks, undertake espionage or sabotage or assist a third party in illegal activities
- Enabling access to data (including technological intelligence, national security information, commercial security information, private data)
- Built in "call home"/ wiretap capability to transfer data or control to another country/group
- Weakness in R&D process – inject person or software threat
- Weakness in supply chain – inject component (pre or post build)
- Weakness in person – bribe
- Weakness in onsite support capability – inject person/bribe or install illegal software

As can be seen by the range of ways and methods technology vendor's hardware and software could be maliciously used requires continuous assessment of the techniques and potential weaknesses to be undertaken. At Huawei we assess all of these items and ask ourselves the question "what would someone need to do to execute one of these attack mechanisms?" We then ask "what would be a cheaper, lower risk, higher probability of success mechanism?" and from these answers we work out how best to mitigate any such event. Our current model is, we assume nothing, we believe no one, and we check everything.

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

Huawei takes a "built-in", not a "bolted on" approach to cyber security risk management. In addressing the requirements of cyber security, we have built into all of our standard processes, baselines, policies and standards the best practice that is required. In this way, cyber security is not something that is an afterthought. Instead, it becomes a standard part of the way we do our daily business – it has become part of our DNA.

However, we accept that just because you have a process that does not mean that it is a good process, or that anyone actually executes the process. To address these issues, we have taken the following actions:

- Huawei has established standardized business processes globally and has identified Global Process Owners (GPOs) for each process and Key Control Points (KCPs). In addition, Huawei has established a Global Process Control Manual and a Segregation of Duties Matrix that are applicable to all subsidiaries and business units. The GPOs are responsible for ensuring the overall internal control effectiveness, in light of changes in operational environment and risk exposures.

- From a governance perspective, there is a standing Board Committee dedicated to cyber security chaired by a Deputy Chairman. On this Board sits the main Board Members and Global Process Owners who have a role in ensuring that cyber security requirements are imbedded in processes, policies and standards and that they are executed effectively. If there is any conflict, or resource issue in cyber security, this committee has the power, remit and seniority to make decisions and change the business without reference to anyone else.

- Huawei Auditors use the Key Control Points and the Global Process Control manual to ensure processes are executed and that they are effective. Audits, external inspections and third-party reviews all validate what is happening against what should happen. Individual personal accountability and liability (the rules and regulations) are built into Huawei's Business Conduct Guidelines and business processes that specify how we must behave in our daily operations. Knowledge is updated through online exams every year to keep knowledge current and this forms part of our Internal Compliance Program.

However, there is nothing more important than allowing your processes and internal systems to be opened up to audit and scrutiny from your customers and from governments. It is this ability to use real customers and experts from many fields and governments to inspect, vet and validate our approach that truly enables us to develop world-class processes and integrated systems. Huawei operates in over 140 countries because it is trusted by customers in over 140 countries. Once again, it is a repeatable process that is also a virtuous circle.

In practice what does this mean? Let us give you an example. Many global technology vendors such as Huawei licence and use software components from many third parties, and this is included within our own developed computer code. Our own software may be developed by multiple teams in multiple countries. Yet when there is a security issue, or vulnerability is found, it is crucial that our internal processes and systems give us the ability to forward and reverse-trace the software components that have been developed and pinpoint what products they are in.

At Huawei, we are continuously enhancing our internal systems and processes to enable us to trace-forward from a raw customer requirement all the way through to the computer code that was produced, and also to reverse-trace from the computer code (or patch/modification) all the way back to the raw requirement that required that computer code to be developed.

Within this, we ensure segregation of duties in the R&D process. Software developers cannot approve the final test results or final release. No software developers can authorise the implementation of their own software as there is an independent rigorous review and sign-off process – once signed off, software is automatically uploaded onto support websites, ready for downloading into manufacturing or customer sites.

However, cyber security is not just about technology. It is also about people, laws, incentives and disincentives. Whilst there is undoubtedly a focus on the design, development and deployment of technology, there is an equal focus on all other processes – human resources, legal, sales, finance, marketing, and supplier management. For instance, in terms of supply chain diversity, 70% of the components used by Huawei come from suppliers outside of Mainland China, with the United States serving as the largest provider at 32% and the majority are high technology components, and Taiwan and Europe combining to provide 32%. To manage supply chain risk, Huawei embed in our Procurement Process security control activities such as supplier security qualification and selection, material security testing, supplier security audit, problem improvement, performance management, risk management, vulnerability management, emergency response, traceability and security agreement. All suppliers should pass our cyber security qualification and sign cyber security agreement. Products from all suppliers should undergo cyber security testing. Service delivery of all suppliers should be accepted in terms of cyber security. Until now, Huawei has signed cyber security agreement with more than 2500 engineering and material suppliers.

At Huawei, because we have built cyber security requirements into our processes, each executive, manager and individual has personal accountability and ownership of their responsibilities. This level of responsibility implies several underlying factors, including continuous training, getting the balance right between incentive and personal liability, and continuous loop-back processes to enhance our capabilities and validate our assurance level. This is the Huawei way of meeting the challenges of cyber security.

At Huawei, we adopt the “many eyes” and “many hands” approach to provide openness and transparency on what we do. We positively encourage audits, reviews and inspections on all technology vendors, including Huawei, in a fair and non-discriminatory manner, as each audit or review enables companies to challenge their thinking, their policies and their procedures, in turn enhancing their capability, product quality and product security. At Huawei, we already provide our customers and governments with the ability to undertake comprehensive validation and verification of our products.

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

Huawei designs and builds our end to end cyber security assurance system for products and services.

During product R&D, Huawei refers to secure development and lifecycle methodologies such as SDL, Open SAMM and SSE-CMM and integrate security assurance activities such as threat analysis and secure coding into our IPD (Integrated Product Development) process. In addition, with reference to CMMI and ISO9000, Huawei builds a comprehensive configuration management system to manage labeling, filing and changes of all deliverables during R&D process. The target is to ensure integrity, consistency and traceability of products and the R&D process.

In terms of technology about products and solutions, based on ITU-T X.805, Huawei builds end to end security of products and solutions. For instance, in product security requirement analysis, in addition to complying with security requirements in product related standards such as 3GPP and ITU-T, we also use threat analysis methodologies like TVRA to carry out threat analysis to identify pertinent security defense requirements; in product development and coding, we refer to secure coding standards of CERT C/C++/Java and secure coding practices of OWASP to formulate Huawei's own secure coding specifications so as to manage Huawei's coding activities; in testing phase, we carry out security testing based on the most dangerous software mistakes in OSSTMM and SANS TOP 25.

As for supply chain management, Huawei establishes the supply chain security management system referring to the instructions and best practices in ISO28001 and ISO28004 and based on our own business requirements. We also include the requirements of C-TPAT into our supply chain security controls. What's more, we refer to ISO31010 and select appropriate risk identification and evaluation instruments according to our management practices. The instruments include: Delphi Method, Failure Mode and Effect Analysis (FMEA), Risk Matrix and Root Cause Analysis etc. Huawei supply chain security management system passed the ISO28000 certification in 2012.

To manage security risks of suppliers, Huawei formulated its procurement cyber security policies, procurement cyber security baseline, security specifications of materials, operational instructions to cyber security system qualification of suppliers, instruments of evaluating the level of cyber security risks of suppliers, table of on-site cyber security evaluation on suppliers, SLA of security vulnerability notification by suppliers and the template of cyber security agreement with suppliers.

In information security management, Huawei bases our information security management system on BS7799/ISO27001 and ISO17799. Huawei information security management system has been certified by BS7799-2/ISO27001 since 2004.

8. What are the current regulatory and regulatory reporting requirements in the United States (e.g. local, state, national, and other) for organizations relating to cybersecurity?

No comment.

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

No comment.

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

No comment.

11. If your organization is required to report to more than one regulatory body, what information does your organization report and what has been your organization's reporting experience?

No comment.

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

The standard agreed by nations, international communities, industry or forums is the foundation for cyber security compliance evaluation on critical infrastructure. Standard organizations should serve as a platform for the communication and consultation of all parties, including authorities, buyers and sellers, to collaboratively improve the standard, evaluation procedures and methodology and ensure the consistency and general applicability of the evaluation result.

Use of Frameworks, Standards, Guidelines, and Best Practices

As set forth in the Executive Order, the Framework will consist of standards, guidelines, and/or best practices that promote the protection of information and information systems supporting organizational missions and business functions.

NIST seeks comments on the applicability of existing publications to address cybersecurity needs, including, but not limited to the documents developed by: international standards organizations; U.S. Government Agencies and organizations; State regulators or Public Utility Commissions; Industry and industry associations; other Governments, and non-profits and other non-government organizations.

NIST is seeking information on the current usage of these existing approaches throughout industry, the robustness and applicability of these frameworks and standards, and what would encourage their increased usage. Please provide information related to the following:

1. What additional approaches already exist?

2. Which of these approaches apply across sectors?

3. Which organizations use these approaches?

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

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

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

7. When using an existing framework, should there be a related sector-specific standards development process or voluntary program?

8. What can the role of sector-specific agencies and related sector coordinating councils be in developing and promoting the use of these approaches?

9. What other outreach efforts would be helpful?

Q1-Q9:

To address cyber security issue, our collective work should be guided by a set of principles to provide a framework for coordination of action to drive progress on an aligned set of strategic priorities and goals, and time-based milestones. We should be prepared to accept that the commitment from some parties may initially not be as strong as we would wish it to be due to the inherent lack of trust between some parties, the issue of local politics and geopolitics, trade protectionism and competitor misinformation – having said that, we should not allow any of these issues to be used as an excuse for not taking action.

Guiding Principles

- IT'S GLOBAL: Efforts to improve cyber security must properly reflect the borderless, interconnected and global nature of today's cyber environment in terms of governance, laws, standards and sanctions
- IT'S THE LAW: Efforts to harmonise and align international laws, standards, definitions and norms must be undertaken, accepting the challenges of cultural differences
- IT'S COLLABORATIVE: Efforts to improve cyber security must leverage public-private partnerships to maximise our chances of increasing our collective ability to thwart attacks
- IT'S STANDARDS-BASED: Efforts to design, agree on and implement international standards and benchmarks of ICT vendors should set the standard based on the perceived risk level – there has to be a balance between security and risk
- ITS VERIFICATION-BASED: Efforts to design, develop and implement global independent verification methodologies that ensure products conform to the agreed standards and benchmarks should be agreed and adopted
- IT'S EVIDENCE-BASED: Efforts to improve cyber security must be based on evidence of risk, evidence of the attacker and evidence of loss or impact – we should focus on facts, not fiction
- IT'S DOING THE BASICS: Efforts to improve basic cyber security "hygiene" must be collectively prioritised to drive the entry point of successful attack to a much higher point

Specific Industry Practices

In addition to the approaches above, NIST is interested in identifying core practices that are broadly applicable across sectors and throughout industry.

NIST is interested in information on the adoption of the following practices as they pertain to critical infrastructure components:

- Separation of business from operational systems;

- Use of encryption and key management;
- Identification and authorization of users accessing systems;
- Asset identification and management;
- Monitoring and incident detection tools and capabilities;
- Incident handling policies and procedures;
- Mission/system resiliency practices;
- Security engineering practices;
- Privacy and civil liberties protection.

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

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

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

4. Are some of these practices not applicable for business or mission needs within particular sectors?

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

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

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

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

9. What risks to privacy and civil liberties do commenters perceive in the application of these practices?

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

11. How should any risks to privacy and civil liberties be managed?

12. In addition to the practices noted above, are there other core practices that should be considered for inclusion in the Framework?

Q1-Q12:

Some of the above-mentioned practices are applied in products and solutions of telecommunication networks. For instance, separation of business from operational systems: according to practices of telecom industry, user plane, signal plane and management plane defined in ITU-T X.805 are usually separated, especially in the practices of core network design and deployment; application of encryption algorithm: in practice, encryption algorithm is essential to achieve security. We require using mature standard commercial algorithms and prevent the use of an algorithm that is not strictly reviewed and approved; as for identification and authorization of users accessing systems, there are AAA,Kerberos, PAP/CHAP/EAP, etc.; security engineering practices: refer to SSE-CMM, SDL and OpenSAMM, etc., in practice; incident handling policies and procedures: in practice, CERT CDT, ISO 30111 and ISO 29147 can be referred to.

Huawei is more than willing to cooperate with the industry in developing standards. Huawei is a substantial contributor to global security standards. For instance, Huawei submits numerous security proposals to 3GPP (The Third Generation Partnership Project) each year. Huawei also takes the lead in developing the H(e)NB security standard and pushes the security research on M2M (Machine to Machine) and PWS (Public Warning System) system together with the main operators and vendors in the industry. Huawei positively encourages its people to be very active in many IETF (Internet Engineering Task Force) work groups such as IPsec, Karp, syslog, OSPF, MPLS, Hokey and IPv6 to discuss IP-related security issues with industry experts and because of this active involvement many improvements to proposed standards have been released. Huawei contributes to the security of virtual networks and the standard of anti-junk information. Huawei is a member of the Open Group whose preliminary criteria for development of a supply chain standard has been adopted by Huawei. Furthermore, Huawei has participated in the security standard activities of organizations such as IEEE (Institute of Electrical and Electronic Engineers), OMA (Open Mobile Alliance), UPnP Forum (Universal Plug and Play Forum) and the WiFi-Alliance.

[i] Donald A. Purdy, Jr., Chief Security Officer, Huawei Technologies USA. Andy.Purdy@huawei.com.