This is the consensus response of the State, Local, Tribal and Territorial Government Coordinating Council (SLTTGCC), and are reflective of our sector. The Council appreciates the opportunity to comment, and would like to continue our input as the framework is developed. SLTT government manages transportation, radio communications, utility delivery and emergency services – all of which are enabled by information technology. Securing this technology has not historically been a priority for SLTT government; however, because of the inventory of services that cut across many critical sectors there is some urgency in deploying adequate control frameworks. It is the hope of the Council that further engagement will lead to the development of a framework that may be implemented in SLTT government to address these important issues.

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?

Funding for acquisition and prioritization of resources as the greatest challenge in SLTT government, as well as a common operating picture on various scales – across a metropolitan region that is a collection of local jurisdictions, for example. Difficulty in attracting and retaining resources is a challenge, as the private sector competes strongly and successfully for these resources.

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

There are many frameworks that have been adopted as standards of practice, and these are all fairly similar. However the scope of these frameworks is different, and to develop a single framework for implementation across sectors means that it would need to cover financial systems, health information, control systems and other infrastructure elements and this is very broad. Typically, the

scope of a control framework is limited to, e.g., systems that process cardholder data (PCI-DSS). Being overly proscriptive on a broad scope of systems would be financially prohibitive. The framework should prioritize the identification of high-risk assets, and make those the scope of the control framework.

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?

Senior management in SLTT government is rarely engaged in these issues, unless a significant event causes bad publicity or loss of service that must be explained. It is this 'management by landmine' that makes the implementation of a voluntary framework quite difficult in SLTT government.

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

In SLTT government, information security is generally part of the IT organization, reporting to the CTO, CIO, or Director of IT. A limited number of jurisdictions have designated a CSO, who reports directly to the Executive.

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

Risk is the product of threat probability and consequence. In cyber terms, threat probability may be parameterized using:

- **the presence of a vulnerability**
- **the existence of exploit code**
- **ease with which attacks may be carried out**
- **whether mitigating or compensating controls are possible to implement**
- **known attacks in progress**

The disposition of identified risk can be avoid, accept, mitigate or transfer. Mitigation plans frequently end up as acceptance or avoidance, and risk transference through insurance is still relatively rare.

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

In SLTT government, risk is generally considered as risk of litigation and bad outcomes (due to things like improperly painted crosswalks). Cyber risk is now being considered as something to transfer - through insurance. This strategy, from the perspective of insurers, is applied at the enterprise level (where an organization would have to demonstrate standards of practice throughout to receive reduced rates). A better way of managing risk through transference is to apply the technique to a target of evaluation such as a control system, rather than the enterprise as a whole.

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

Risk management frameworks derived from standards of practice such as ISO27001/2; the PCI-DSS; the NIST 800-53 framework, and others. Tools used in SLTT governments for tracking risk are generally spreadsheets.

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?

In SLTT governments, the only regulatory requirement to report is via State breach reporting statutes. There are occasional audits for PCI and HIPAA compliance; CJIS for law enforcement and NERC if an energy utility is involved. An oblique exception to this is auditing against a standard (pulled from the air, apparently) for insurance risk pool members. This is good, because it is using a market force to apply security controls, and bad because it is somewhat arbitrary and inconsistently applied.

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

Critical assets are control systems - dependent on energy and telecommunications/IT and emergency services - dependent on transportation, energy, telecom, IT and water. Good example guidance on this can be found in the Emergency Services Sector Cyber Risk Assessment April 2012, which spent considerable effort on identifying dependencies.

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

Service provision trumps IT security in most cases, and financial considerations receive more of an audience than does risk management in SLTT governments. Performance goals are generally focused on "uptime" and management of constituent perceptions.

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?

SLTT governments are not generally regulated, nor do they report unless required through public disclosure or through breach notification, apart from regulated agencies (e.g. Water, Energy).

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

Rather than standards for application of control frameworks to network operations, these organizations should focus on the security of Internet protocols. Ideally, the protocols that underpin Internet traffic should be brought into this century - they were developed specifically for openness, and are a hindrance to securing the network. VoIP standards similarly need updating, for example a system that would register the IP address of a VoIP device, so that CLID spoofing would be traceable back to an ISP customer. As far as standards for controls are concerned, there are many already in

existence and production of yet another would not significantly change anything. NIST 800-53 is voluntarily applicable today.

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?

ISO 27001/2; PCI-DSS; NIST 800-53; the FFIEC audit handbook and guidance from the OCC; the Information Security Forum's standard of good practice; the ten domains of the common body of knowledge from ISC2; the COBIT framework; capability maturity models - mainly from Carnegie-Mellon.

2. Which of these approaches apply across sectors?

The ISO standard, NIST 800-53, ISC2 CBK - in fact most of them can be applied to just about any sector.

3. Which organizations use these approaches?

ISO certification is rare, as there is little competitive benefit (today). PCI is in wide use due to the ubiquitousness of credit card transactions. NIST 800-53 is used mainly in the federal government, but used as a framework to build upon in the private sector.

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

There is little benefit to voluntarily spending to implement these frameworks, as nearly all are reduced to checklists when implemented.

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

Specify outcomes rather than controls. For example, minimizing the residence time of malware compromises on key assets.

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

Those that are sector-specific focus on key assets in that sector. For example NERC-CIPs focus on the bulk electric system, electronic perimeter, and areas where the impact would be in excess of 300MW.

The FFIEC and OCC guidance apply to financial transaction systems and focus on many insider issues. SLTT governments are so diverse, with so many levels of education within the sector that pressing frameworks, guidelines and best practices without offers of educational assistance could be counterproductive within the smaller jurisdictions.

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

One size will definitely not fit all, so sector-specificity is likely required. However, parts (if not all) of any of these frameworks may be deployed today - there has never been a barrier to adoption, apart from the uncertain ROI on that adoption. Empirically, it becomes a solution in search of a problem unless an organization has extremely valuable information (intellectual property, e.g.) to protect, or has experienced a bad outcome with disruption or theft through logical (cyber) means.

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

Demonstrate the "right touch" on application of an existing standard to a specific sector. "Here is how we recommend the NIST 800-53 framework is deployed in the water sector", for example.

9. What other outreach efforts would be helpful?

SLTT governments require outreach. The scale at which disruption is likely to occur is local, not national. Metropolitan areas that are a collection of local jurisdictions that share network connectivity, radio communications, transportation management and emergency services need to address these areas, as the impact of disruption is likely to be loss of life. The issue is NOT credit cards and "data breaches", and they need that message.

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?

In SLTT government they are applied as-needed to solve a business problem, create efficiencies, and reduce redundancy and improve automation. Some are adopted because of regulatory oversight (mainly from the payment card industry).

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

The international standards are not proscriptive, e.g. "encrypt sensitive data while stored", without specifying algorithms or products. However all are covered by existing standards and frameworks.

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

NOTE that preventive controls DO NOT WORK when adversaries are so well-resourced and determined. A focus on detection and rapid response is warranted. Identification and authorization of users accessing systems; Monitoring and incident detection tools and capabilities; Incident handling policies and procedures are all very aligned with that focus. We would add that policy controls are very important, for example a prohibition on mixing sensitive operations with routine e-mail and web use on the same system.

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

Encryption is mainly used to protect information that is regulated, or business-sensitive (intellectual property). Encryption and key management are expensive and not widely used in SLTT governments apart from messaging security.

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

Encryption is difficult to implement, as is mission/system resiliency practices (as this is not a familiar term like continuity of operations).

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

Mainly the standards provide guidance as to where the practices may be applied (for example, information of a certain classification level must be encrypted while stored).

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

Most SLTT organizations have information security policies, standards and guidelines and these should be reviewed annually. This is a standard work plan item for IT leadership.

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

Most do not.

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

A focus on detection and response means a good deal of activity monitoring. This is not necessarily a risk to privacy, as it can be done without identifying information.

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

The Canadian (PIPEDA) and European (Safe Harbor) regulatory requirements would be aligned with the adoption of these standards and frameworks, and in fact require demonstration of compliance with at least a subset. This would allow information flow between Europe and the US, and Canada and the US to proceed at an increased rate of flow, which would presumably help private sector business.

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

Through anonymization of summary monitoring data. Leave usernames out of the logs.

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

A requirement to report events of a certain, pre-negotiated taxonomy to the State fusion center, for adjudication as to whether information should be shared state-wide, escalated into federal visibility, etc.