February 5, 2018

**Agriculture and Agri-food Canada   
2017 Cyber Security call for input**

The National Strategy and Action Plan for Critical Infrastructure by Public Safety Canada established a collaborative government (federal, provincial, territorial) and industry sector approach to mitigate the full range of risks and threats facing vital assets and systems. The agri-food, including fisheries, supply chain is one of the 10 identified critical infrastructure sectors.

The National Strategy recognizes that critical infrastructure owners and operators have the expertise and information that governments need to develop comprehensive emergency management plans and, in turn, that governments have information on risks and threats that are relevant to owners and operators in carrying out their risk management activities.

In the spirit of the Strategy, Agriculture and Agri-food Canada (AAFC) has prepared this call for input in collaboration with the Canadian Supply Chain Food Safety Coalition and the Canadian Animal Health Coalition, to gauge current awareness levels and obtain information on possible cyber issues/threats affecting the food sector: how they may occur, as well as the sector’s readiness for such threats. This call for input will help AAFC support the sector’s readiness by providing pertinent and timely information to support planning. It will also help the Government of Canada assess and understand the current cyber security threats to the sector.

For any questions on this questionnaire, including content, intent and format, or any related feedback please do not hesitate to contact [AgEM-GUAg@AGR.GC.CA](mailto:AgEM-GUAg@AGR.GC.CA). AAFC will consolidate the feedback and use it to inform efforts to improve the policies, programs and services in support of cyber security in the food sector.

|  |  |
| --- | --- |
| **Date**: |  |
| **Organization name**: |  |
| **Contact information**: |  |

1. Please check the box that best describes your organization:

|  |  |
| --- | --- |
| National association | Individual company |

1. Please check all boxes that best describe your organization’s segment of the supply chain:

|  |  |  |  |
| --- | --- | --- | --- |
|  | Primary production |  | Importer |
|  | Processing |  | Exporter |
|  | Manufacturing |  | Other (please specify) |
|  | Handling/distribution |  |  |
|  | Storage |  |  |
|  | Transportation |  |  |
|  | Retail |  |  |
|  | Food service |  |  |

1. Please answer the following questions regarding your organization:

* Number of employees:
* Geographic distribution:
* Annual revenue (optional):

|  |
| --- |
| $0 - $500,000 |
| $500,000 - $1,000,000 |
| $1,000,000 - $5,000,000 |
| $5,000,000 - $10,000,000 |
| $10,000,000 - $50,000,000 |
| Other |

1. Please check all boxes that best describe how your organization manages information technology management and support:

|  |  |
| --- | --- |
|  | All in-house (fully staffed from an IT perspective and self-sufficient) |
|  | Managed in-house (IT capabilities outsourced including desktop, network services, monitoring, application development, and maintenance) |
|  | Some in-house support |
|  | Mostly or all out-sourced |

1. Public Safety Canada’s Canadian Cyber Incident Response Centre (CCIRC) assists critical infrastructure organizations, businesses and provincial/territorial/municipal governments in Canada to protect their cyber systems from compromise. Additionally, they act as a point of contact to report cyber incidents and obtain advice on cyber security from the Government of Canada. How aware is your organization of CCIRC?

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **1** | **2** | **3** | **4** | **5** |
| Never heard of CCIRC | We have heard very little about CCIRC | Somewhat aware of CCIRC | We have heard about CCIRC but do not know how to use their services | We are very aware of CCIRC and/or have used their services |

1. There are various types of cyber threats that can affect the agriculture, fisheries and food sector computer networks. These include botnets, hacking attempts, malware intrusions, phishing, ransomware attacks, spam and viruses among others. Has your organization ever faced a disruption or destruction of any kind on any operational (control systems)/corporate networks or systems within the last two years?

|  |  |
| --- | --- |
| No | Yes |

More than two years ago?

|  |  |
| --- | --- |
| No | Yes |

1. If you answered yes to the question above, please explain what cyber threat(s) your organization has experienced and how your organization responded to and mitigated these threats.
2. As seen in Question 6, there are a variety of cyber related risks which can affect both corporate PCs and internet-enabled computers and devices, that, if compromised, can be affected or may become a vector affecting other parts of your system. These include many common devices such as servers, desktops, computers, mobile phones and smart devices, tablets, websites, and smart TVs. Does your organization have methods or protocols in place to protect these systems and devices? Please list them below.

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

1. What are the types of information your organization is most interested in protecting that could cause financial or reputation damage if compromised?

|  |  |
| --- | --- |
|  | Personal information about your employees |
|  | Information about your members, customers, service/product suppliers |
|  | Intellectual property |
|  | Important data related to your business practices and strategies |
|  | Other (please specify) |

1. Please check all the cyber systems that your organization uses:

|  |  |
| --- | --- |
|  | Production Control Systems |
|  | Point of Sale Systems |
|  | Global Positioning Systems |
|  | Radio-Frequency Identification Systems |
|  | Traceability Data Systems |
|  | Other (please specify) |
|  |  |

1. Are you comfortable with your organization’s ability to detect, respond to, and mitigate cyber incidents/threats?

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **1** | **2** | **3** | **4** | **5** |
| Don’t know | No | A little | Yes, only for small incidents | Yes |

1. Does your organization provide ***physical*** security awareness training for employees?

|  |  |
| --- | --- |
| No | Yes |

1. **Does your organization provide *cyber* security awareness training for employees?**

|  |  |
| --- | --- |
| No | Yes |

1. What information would you find useful to receive from the Government of Canada’s cyber security experts (such as CCIRC) to support your planning and preparedness for cyber-attacks? Check all boxes that apply.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Bulletins |  |  | |
|  | Targeted briefings |  |  | |
|  | Training |  |  | |
|  | Other (please specify) |  | |  |

1. ***How*** is your organization currently made aware of cyber threats/incidents? Check all boxes that apply.

|  |  |  |  |
| --- | --- | --- | --- |
|  | Bulletins |  |  |
|  | Targeted briefings |  |  |
|  | Training |  |  |
|  | Other (please specify) |  |  |

1. ***From whom*** is your organization currently made aware of cyber threats/incidents? Check all boxes that apply.

|  |  |
| --- | --- |
|  | ISP Providers |
|  | Governments |
|  | Industry associations |
|  | Technical Support Providers |
|  | Other (please specify) |

1. Do you have a cyber plan established for your organization that covers the Emergency Management pillars of prevention/mitigation, preparedness, response, and recovery?

|  |  |
| --- | --- |
| No | Yes |

1. Do you currently use firewalls or virus detection software or services on your networks?

|  |  |
| --- | --- |
| No | Yes |

1. Do you currently have protocols established for regular employee password changes?

|  |  |
| --- | --- |
| No | Yes |

1. How aware is your organization of the following cyber security standards/documents?

**National Institute of Standards and Technology – Cyber Security Framework**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ☐ **1** | ☐ **2** | ☐ **3** | ☐ **4** | ☐ **5** |
| Not at all | Very little | Somewhat aware | Aware | Very aware |

**International Organization for Standardization**

* **27001 - Information Security Management**
* **27032 - Guideline for Cyber Security**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **1** | **2** | **3** | **4** | **5** |
| Not at all | Very little | Somewhat aware | Aware | Very aware |

**Additional Comments or Suggestions**

Please include any comments or suggestions that you would like to share.

*Response:*

Thank you for your feedback. Please provide completed forms by **March 1st, 2018** to:

AgEM-GUAg@AGR.GC.CA

To report a cyber threat or incident, please contact [ps.cyberincident-cyberincident.sp@canada.ca](mailto:ps.cyberincident-cyberincident.sp@canada.ca), free of charge, 24/7. For more information on cyber security, please visit <https://www.publicsafety.gc.ca/ccirc>.