ANNEX - *Supporting Context for Cyber Incident Information Collection by Law Enforcement*

Cybercrime Investigation Support - Victim Engagement Questions from Law Enforcement

Statement of Purpose:

At the outset of collecting information pursuant to these questions, both the querying law enforcement officer and the complainant reporting to law enforcement will share a common understanding of the underlying purpose behind this line of engagement. The document and its questions are a product of consultations and extensive input from cyber experts from both law enforcement and legal counsel who respond to cyber incidents on a regular basis.These objectives are: *For a law enforcement officer to collect information relating to a possible criminal offence against a cybercrime victim. Information requested is intended for the purposes of supporting cybercrime reduction, enabling resources to provide support to victims and to not, in any manner, seek to gain access to any information that would be subject to privilege. These objectives are met through and intended for:*

1. *The identification of those suspected of conducting criminal activity against cyber systems which victims depend on;*
2. *The gathering of evidence against those suspected criminal actors for the purposes of potential eventual arrests, charges and prosecution;*
3. *Providing details that may contribute to law enforcement activities intended to disrupt current and future cybercriminal actions;*
4. *For the purposes of supporting all law enforcement and associated prosecutorial processes against cybercriminals; and*
5. *For the purposes of allowing law enforcement to best support victims of cybercrime during their time in need and fostering connectivity between victims and available resources/supports which may be of assistance.*

Critical Information Requirements for Law Enforcement:

From the outset of engagement between the investigator and victim, it is possible there could be some hesitation in the victim's willingness to provide the information that law enforcement is requesting. This apprehension may be due to a lack of familiarity with exactly what to expect during the course of an investigation against the criminal actor who victimized them. It could also be as a result of, at some point in their cyber incident response process, an assessment of risk was made that relates to sharing information of their breach with anyone external – including law enforcement. Regardless of the source, the document *WHAT TO EXPECT DURING THE ONSET OF A CYBERCRIME INVESTIGATION* may be useful to refer the victim to early in the engagement process, even in advance of first contact between the investigator and victim.

To ensure full transparency of intent, victim organizations and those reporting cyber incidents to law enforcement should understand what information law enforcement agencies are looking to obtain from them. The intent of information sought relating to the cyber incident ensures that any associated parties

engaging in the investigation, prosecution and/or incident response-related activities are able to perform their duties and functions.

These information requirements support the activities of law enforcement agencies to pursue actions against criminal actors and should not constitute anything construed as subject to privilege. The critical information requirements that form the basis of the information sought within this questionnaire include:

1. Victim organization identification and contextual information;
2. Facts relating to the incident and associated severity impacts – including number of effected endpoints and other factors;
3. Attack vectors;
4. Accounts and attributions to threat actor(s);
5. Key virtual currency addresses and activities related to the incident;
6. Relevant log files on the network/host; and
7. Indicators of compromise and other observed tactics, techniques and procedures.

Provision of Information Process:

The *Cyber Incident questions from Law Enforcement* use a two-phase approach for information to be shared from a victimized organization to law enforcement. The specific questionnaire will be used by law enforcement to obtain information through a trusted and victim-friendly engagement process using two phases.

Phase 1 will consist of six concise questions that represent both the most immediate and critical information requirements by law enforcement in order to initiate an appropriate law enforcement response.

Phase 2 will consist of a request for a combination of more detailed follow-up information and/or information that is more supportive or peripheral context to the incident.

It is possible, if resources and availability from the complainant are available at the time of initial contact, for both Phase 1 and 2 information to be provided at once. As a general rule, Phase 2 information will be provided in a follow-up manner as the incident progresses as complainant availability permits and information becomes available and/or evolves with the incident.

Phase One Reporting Information

1. *Information relating to the reporting individual/complainant*
   Intent: Reporting individual/organization provides information to identify themselves, provide key contact information for follow-up and outline their relationship to the cyber incident. (Examples include the name of complainant, title or position/association to the victim, contact information).

2. *Information relating to the victim of the incident*

Intent: Reporting individual provides information to identify the victim organization and associated information that will support law enforcement in assessing issues such as jurisdiction and potential coordination requirements with other law enforcement agencies.
(Examples include name of organization, address, key functions and/or services of the organization. Other contextual information to assist context includes, if applicable, critical infrastructure sector/sub-sector, corporate structure and, if applicable, associated geographic locations of the organization.

3. *Key details outlining the incident*
Intent: Information reported is intended to provide important context to understand the type of incident that has occurred along with the corresponding scale, scope and impact. This information provides details to situate the type of criminal activity which has occurred and important considerations relating to the severity of the crime. These details can also provide valuable contextual information that could potentially establish links to previous criminal activity. It is acknowledged that some of this information may be considered sensitive to the victim organization at this time and sharing should remain within the comfort level of the victim. In the event that specific information is required from law enforcement for purposes of addressing immediate issues of public safety, that should be communicated by the law enforcement official to the victim along with the appropriate context.
Examples of information include the following:

- **a.** *Overview of occurrence – preliminary information (i.e., known to date) relating to what has happened (e.g., data breach, ransomware, DDOS) and associated details relating to what has been impacted;*
- **b.** *A general description of operations affected by this incident – (e.g., a high-level overview – provided to a level of specificity that the victim organization is comfortable with – that may include a description of services and/or number of employees impacted, extent of impact and services still available at full capacity at time of reporting);*
- **c.** *Incident timeline – preliminary information such as key aspects of the incident timeline that can be shared at this stage (e.g., when was the incident first discovered, evolution of the incident and current status);*
- **d.** *Known consequences of impact – Initial assessment relating to the impact's level of jeopardy to the extent that the victim organization is willing to share at this juncture. Law enforcement's more immediate concerns relate to determining if there is any known risk to public safety as a result and/or occurring or anticipated risk to critical infrastructure (negative impacts on public safety, organization's finances, regional/national economic, critical services, downstream impact on customers/supply chain, etc.).*

4. *Threat vector details*
Intent: Information collected is intended to provide law enforcement with details that may correlate the occurrences of the incident with the activities of threat actors engaged in criminality against the victim. Note that more technical and/or detailed information will be collected during Phase 2. Information collected is intended to be of a preliminary nature only

and could assist law enforcement in determining if there is any immediate danger associated with an incident in progress.

Examples may include any occurred or current direct contact with the threat actor up to and including at the time of reporting.

5. *Other incident related information not yet provided*
   Intent: Information relating to the incident is all important, no matter how trivial the complainant or victim may consider it. For example, is there any further information at this time which could assist law enforcement with a deeper understanding of the incident?

6. *Key contact information*
   Intent: Based on the information collected at initial reporting through Phase 1, a law enforcement agency may follow-up to obtain further information in support of a criminal investigation or other law enforcement directed activities that may be associated with the cyber incident reported. The victim organization should identify any key points of contact for law enforcement agencies to follow-up and discuss the incident in greater detail. These contacts may include individuals supporting the incident response process from external public and/or private sector organizations such as legal firms (including breach coaches), insurance firms, banks, Computer Security Incident Response Teams and/or the Canadian Centre for Cyber Security.

Phase Two Reporting Information

1. *Incident Response Associated Information*
   Intent: Information collected is intended to complement with greater, and potentially more technical, detail than what was provided during Phase 1 reporting in section 3 – details outlining the incident. As in the previous phase, the information may be considered sensitive and law enforcement should be mindful of this and communicate why providing these details supports the investigation, will be used in that context only and not be released by law enforcement to the public. There is a high likelihood that aspects of the crime committed against the victim will correspond with tactics, techniques and procedures used against other victims and these requested details may be valuable for law enforcement to make these cross jurisdictional linkages in pursuit of the bad actors. Requested information at this stage may include, as available, details such as the following:
   - **a.** *More specific details relating to the incident timeline and extent of compromise;*
   - **b.** *Details relating to the intrusion known to date – including indicators of compromise and tactics, techniques and procedures employed to gain access and infiltration;*
   - **c.** *Relevant log files on the network relating to the incident;*
   - **d.** *Preliminary incident response report (if/when available).*

2. *Threat vector details*
   Intent: Information collected is intended to provide law enforcement with details that may correlate the occurrences of the incident with the activities of threat actors engaged in

criminality against the victim. In some instances, especially if there is ongoing engagement with the threat actors, some information provided could potentially provide immediate correlated value that would allow law enforcement to share mitigation and/or response details which may be useful for the victim organization to consider in it incident response process.

Examples may include noted contacts with the threat actor such as details relating to business email compromise, phishing, and/or ransom-related demands. This may include, as available, details such as the following:

- **a.** Attack vectors;
- **b.** Contact with threat actors – communication(s) and/or transactions
- **c.** Accounts and attributions to threat actor(s);
- **d.** Key virtual currency addresses and activities related to the incident;

3. *Ransomware Incident Specific Information*
It should be noted that victim organizations may be hesitant to engage with law enforcement on the subject of paying ransom. The law enforcement official engaged should be sensitive and reassuring that, while law enforcement does not support paying ransom to the cybercriminal actors as it provides a further enabler to cybercriminal activity, it is recognized that the victim organization has the right to manage risk to its continuity of operations and make decisions accordingly. Information provided relating to engagement with the threat actors and any related information associated with the paying of ransom will not be used by law enforcement against the victim and only for supporting investigation against the cybercriminal actor.
Information requested may include:

- ***a.*** *Additional data artifacts related to the incident (e.g. Ransom note, Bitcoin Wallet ID, email, monikers, phone calls, suspicious IPs, malicious files, log files, etc.).*
  (NOTE: It helps when the location of the files is properly sourced: Computer location, name, file path, and creation date – if available this information is helpful for law enforcement-related activities.)
- ***b.*** *Has a ransom been paid?*
  - ***i.*** *If so, any details associated with the payment including any key virtual currency addresses and activities related to the incident.*
  - ***ii.*** *If considering payment, process-related information associated with the upcoming transaction.*
    (Note: Information relating to the decision to pay ransom is not required for law enforcement)

4. *Other incident related information not yet provided*
Intent: Information relating to the incident is all important, no matter how trivial the complainant or victim may consider it. Is there any further information at this time which could assist law enforcement with a deeper understanding of the incident?