PEMA CYBER EVENT INFORMATION CHECKLIST

See page 3 for additional guidance and information

Item #		REQUESTING AGENCY INFORMATION	
1.	A.	Local Task Assignment / Mission / Incident / Event Number:	
	B.	Jurisdiction:	
	C.	Requestor Lead POC Information:	**(Name, Phone #, Email)**
	D.	Does the jurisdiction have a Cyber Event Response plan? **If YES, Email the plan to stateeoc@pa.gov.**	◯ **YES** ◯ **NO**
	E.	Location of the event:	**(Street address, Town, County)**
2.	◊	**ESSENTIAL ELEMENTS OF INFORMATION (EEI)**	
	A.	**Did this event result in a Proclamation of Disaster (IAW Title 35 Pa.CS 7301(c) at the Local Municipality or County level?**	◯ **YES** ◯ **NO**
	B.	**Is the reporting agency's Chief Information Officer (CIO) aware of the situation? What is his / her recommendation(s)?**	◯ **YES** ◯ **NO**
	C.	**Is your EM / 911 Network or Call Center affected? If YES, how? (Explain in Notes)**	◯ **YES** ◯ **NO**
	D.	**Is there an articulated imminent threat to the citizens of the Local Municipality, County, or Commonwealth?**	◯ **YES** ◯ **NO**
	E.	**Is this event likely to jeopardize life, endanger public health or the economic stability of the Commonwealth through a loss of the integrity of critical infrastructure and key resources?**	◯ **YES** ◯ **NO**
	F.	**Does this event cause the implementation of COOP / COG processes at the Local / Municipality, County, or Commonwealth level?**	◯ **YES** ◯ **NO**
	G.	**Does this event pose a significant impact to safety and security; energy; communications; transportation; food, water, sheltering; hazardous material; health and medical lifelines?**	◯ **YES** ◯ **NO**
	H.	**Is the Jurisdiction's Insurance Company, Mutual Aid, or Procurement Process notified or used?**	◯ **YES** ◯ **NO**
	I.	**Is this network part of, or connected to, the State Enterprise Information and Communication Technology Systems?**	◯ **YES** ◯ **NO**
3.	□	**INFORMATION REQUIREMENTS (IR)**	
	A.	Does the agency have any external support from insurance provider(s) / private vendor(s) / contractor(s) that assist with information security and remediation? **(Explain in Notes)**	◯ **YES** ◯ **NO**
	B.	Has supporting agencies and partner stakeholder been advised of the event? (Including, PaCIC, PA Office of Homeland Security and other federal or commonwealth agency who support is needed to respond, investigate, mitigate or recover from incident)	◯ **YES** ◯ **NO**
	C.	Who is the Incident Commander or the lead Point-of-Contact (POC) for the reporting agency?	**(Name, Phone #, Email)**
	D.	Has agency security or local, county, or commonwealth law enforcement (e.g. PA State Police) been notified? (Explain in Notes)	◯ **YES** ◯ **NO**
	E.	Have any measures been taken to preserve evidence (e.g. logs and records)? **(Explain in Notes)**	◯ ◯ **NO**
	F.	Is the potential compromise of public or private information likely or probable?	◯ **YES** ◯ **NO**
	G.	Has the network been isolated / contained?	◯ **YES** ◯ **NO**
	H.	Has a root cause analysis been initiated or determined? **(If DETERMINED, explain in Notes)**	◯ **YES** ◯ **NO**
	I.	Are there any MOUs in place with other Commonwealth Agencies? **If YES, Email the plan to stateeoc@pa.gov.**	◯ **YES** ◯ **NO**

PEMA CYBER EVENT INFORMATION CHECKLIST

See page 3 for additional guidance and information

Item #		CURRENT RESPONSE / MITIGATION OPERATIONS
4.	A.	Have corrective actions have been planned or initiated? **If YES, what actions? (Explain in Notes)**
	B.	What essential, or critical, functions cannot be performed? **(Explain in Notes)**
	C.	What is your response and restoration priorities? **(Explain in Notes)**
	D.	Have recovery processes, tactics, goals and objectives been determined? **(Explain in Notes)**
5.	Item #	NOTES

PEMA CYBER EVENT INFORMATION CHECKLIST

See page 3 for additional guidance and information

This form should accompany a completed PEMA Resource Request form and be sent to PEMA CWWC via email (stateeoc@pa.gov) and PEMA Logistics via email (slogistics@pa.gov). For life-saving requests, a verbal request via telephone or other communication device is sufficient with a follow-up PEMA Resource Request form and a Cyber Event Information Checklist form within 30 days.

Timely submission of this information enables a rapid response to this Resource Request. This worksheet informs the decision-making process by providing Essential Elements of Information (EEI). It also informs Situational Awareness by providing Information Requirements (IR). This initial information will support the four Cyber Event Response lines of effort (Communications, Response, Investigation, and Mitigation) leading to a successful recovery and return to normal operations.

The Archer Reporting Form is used to respond to IT Security Incidents by all agencies, offices, bureaus, commissions, and boards under the jurisdiction of the Governor's Office. (PA Office of Administration Information Security IRP v2.11, February 4, 2019)

1. **REQUESTING AGENCY INFORMATION:**
   - **A.** *Local Task Assignment / Mission / Incident / Event Number* - Provided by Local Jurisdictions assigned task number for tracking request.
   - **B.** *Jurisdiction* - The municipal, county, or state agency providing information regarding the cyber event.
   - **C.** *Requestor Lead POC Information* - Needed for operations, planning and resource coordination.
   - **D.** *Cyber Event Response Plan* - Needed to facilitate situational understanding, operations, planning and resource coordination.
   - **E.** *Location of the event* - Needed for geo-location (Street address, Town, County).

2. **ESSENTIAL ELEMENTS OF INFORMATION (EEI):**
   - **A.** *Proclamation of Disaster – May enable appropriate authorities and resource capabilities.*
   - **B.** *Chief Information Officer (CIO) awareness - Identification of remediation activities and recommendations.*
   - **C.** *Emergency Management / 911 Network affect - This is a critical capability which may be response priorities.*
   - **D.** *Imminent Threat – If an "imminent threat" is articulated, certain processes, authorities and resource capabilities are enabled.*
   - **E.** *Effect on life, health, economic, and CI / KR - If an "effect" is quantified, certain processes, authorities and resource capabilities are enabled.*
   - **F.** *COOP / COG - Implementation of COOP / COG plans for the subject agency may affect stakeholders.*
   - **G.** *Effect on Community Lifelines - If an "effect" potentially impacts a community's lifeline, certain processes, authorities and resource capabilities are enabled. See FEMA Community Lifelines Toolkit.*
   - **H.** *Insurance company, Mutual Aid or Procurement Process - Required to ensure proper coordination.*
   - **I.** *State Enterprise Information and Communication Technology Systems (See Ref 2, TBP) - If the affected network is an element of the State Enterprise, certain processes, authorities, resource capabilities are enabled.*

3. **INFORMATION REQUIREMENTS:**
   - **A.** *External Support - Identify what support, external to the Agency, is being provided. Explain in the notes.*
   - **B.** *Stakeholder Awareness - Are partners and stakeholders aware of the situation?*
   - **C.** *Lead POC - Identify who the IC or Lead POC is.*
   - **D.** *Appropriate LE authority - Has the appropriate law enforcement authority been advised of the situation?*
   - **E.** *Preservation - Have measures been taken to preserve historical information which may assist with attribution and forensic analysis? Explain in the notes as needed.*
   - **F.** *Potential unauthorized disclosure - Has any information been compromised?*
   - **G.** *Contained - Has affected parts of the network been quarantined to prevent further impact?*
   - **H.** *Root Cause - Has a root cause analysis been conducted that would assist forensic and attribution processes of the LE community that was notified?*
   - **I.** *Other MOU's - Are there MOUs that are in effect with supporting agencies, or agencies that cannot now be supported by the affected agency?*

4. **CURRENT RESPONSE OPERATIONS:**
   - **A.** *Corrective actions - What corrective actions are underway to mitigate the effects of this event?*
   - **B.** *Critical Functions - What critical functions can the agency no longer perform because of this event?*
   - **C.** *Response Priorities - What is the priorities that guide the response?*
   - **D.** *Tactics, Goals, and Objectives - What are the incident goals and objectives and how are they being met?*

5. **NOTES:** Provide information as required and for your free text descriptions and statements.

PEMA CYBER EVENT INFORMATION CHECKLIST

See page 3 for additional guidance and information

- **REFERENCES:** References provided to aid in the response and recovery from this event.
- **EMAIL CONTACT LIST:** A list of POCs with which to communicate with and send this report to. Use every POC in the "To" line of an email message.

REFERENCES	
1.	Title 35 PaCS Health and Safety §7301(c) Declaration of disaster emergency.
2.	PA Cyber Incident Annex (DRAFT)
3.	PA Office of Administration Information Security Incident Response Procedure (IRP) v2.11
4.	PA Office of Administration IT Security Incident Reporting Policy (AUG 12)
5.	PA Office of Administration Policy and Procedures for Protecting Commonwealth Electronic Data (NOV 07)

EMAIL CONTACT LIST
PEMA Director
PEMA, Executive Deputy Director
PEMA Director of External Ops
PEMA Division Chief, Logistics
PEMA Director of Internal Ops
PEMA Director, EM Tech Services
PEMA IT Generalist Administrator
OA Policy Analyst 2 - Exec Offices
OA Chief Information Security Officer
OA IED-DC Chief Info Sec Off (Acting)
OA EISO Risk Manager
DMVA PA National Guard, DCOE
Gov Off
GOHS
GOHS
PSP (Sp-protectpa@pa.gov)
PSP Analyst (Sp-watchcenter@pa.gov