THE STATE
of ALASKA
GOVERNOR MIKE DUNLEAVY

Department of Military and Veterans Affairs

Division of Homeland Security and Emergency Management

P.O. Box 5750
JBER, AK 99505-0800
Main: 907.428.7000
Fax: 907.428.7009
www.ready.alaska.gov

May 11, 2021

The Honorable Senator Myers
State Capitol Room 510
Juneau AK, 99801

Dear Senator Myers,

The sponsor of HB 3 – Definition of Disaster "Cybersecurity" relayed the following questions to our department:

Since DMVA is supposed to help with the planning and to some degree mitigation, are there timetables that need to happen between an incident and the declaration of a disaster? In the case of Cybersecurity, if there's a credible imminent threat, are there any guidelines that the department would use? I'm assuming CISA's.

There are no specific timetables between incident and declaration. When a local jurisdiction declares a disaster under A.S. 26.23.140, and the jurisdiction requests State assistance (or when a state agency reports an attack or imminent threat of an attack and the Commissioner of DOA certifies per the bill), the Division of Homeland Security and Emergency Management will take that request, evaluate, and develop what we call a Fact Sheet to provide to the Governor's Disaster Policy Cabinet (DPC). Depending on the circumstances, that factual information may take time to develop. The DPC then formulates a recommendation to the Governor as to whether or not a disaster emergency should be declared. This in no way hinders response actions from taking place. Often times, the declaration is put in place to either facilitate mutual aid response from other states through the Emergency Management Assistance Compact, or to facilitate disaster reimbursements through the Disaster Relief Fund. Of note, FEMA's regulations under 44 CFR 206 place a 30-day time limit from the incident to request federal assistance. We typically ask for a 30-day extension to that requirement, in order to conduct a joint federal/state preliminary damage assessment, which is required when requesting federal assistance.

A "credible imminent threat" would be based largely on intelligence or advanced warning from the federal Intelligence Community, which would include CISA, FBI, US-CERT (US-Computer Emergency Response Team), DPS, and local law enforcement and their IT security partners. That threat intelligence would be vetted with the Chief Information Security Officer and Commissioner of Administration to aid in the certification process.

They have questions about the Alaska Court Systems recent cyber security attack. Hypothetically, if they were to request a declaration for an emergency, what would be the criteria that the State would use to make that determination? Are there regulations that clarify that, for example, FEMA or CISA's guidelines will be the ones used?

Often times the assessment of threats or occurrences of disaster situations relies on subjective analysis. In general, we would use intelligence information as stated above, and the weigh the impacts or potential impacts to physical infrastructure (servers, routers, datasets, etc.) in the context of FEMA's Public Assistance Program and Policy Guide (PAPPG) (https://www.fema.gov/sites/default/files/documents/fema_pappg-v4-updated-links_policy_6-1-2020.pdf). We refer to this document in Alaska's Public Assistance Administrative Plan. The FEMA PAPPG describes a pyramid of eligibility, which includes eligible applicants, work, facilities, and costs. For example, private, for-profit companies are not eligible for disaster assistance. So, if the attack caused damage to facilities within the private sector (contracted server farms, private for-profit SCADA systems, etc.), the costs to repair or replace those facilities would not be eligible. However, if the State of Alaska was required to take what's known as Emergency Protective Measures (emergency procurement of firewalls, emergency contracting of IT responders, etc.) those costs could be eligible. In addition, we would look to CISA's list of Critical Infrastructure (https://www.cisa.gov/critical-infrastructure-sectors) to determine whether the systems or datasets would be considered critical. Often times, the IT systems and backbones utilized to manage utility infrastructure are considered CI. State Executive, Legislative, and Courts are critical governmental functions. The loss of a webserver that provides static, public-facing information about a program wouldn't be considered critical. The Division and DPC will also analyze the incident with respect to the "widespread and severe" portion of the definition. Many factors are weighed there, including impact to life, safety, public health, and property damage, how many areas of the state are impacted, etc.

Please don’t hesitate to contact me with any further questions.

Sincerely,

Bryan Fisher, Director (Acting)
Division of Homeland Security & Emergency Management