Department of Public Safety
Office of the Provincial Security Advisor

Ministère de la Sécurité publique
Bureau du conseiller provincial en matière de sécurité

Working Together for a Safe New Brunswick
Travaillons ensemble pour un Nouveau-Brunswick en toute sécurité

Date: 17 November 2020 To: New Brunswick Owners of Critical Infrastructure, NB Emergency Measures Organization, New Brunswick Police Forces, Fire, Ambulance and 911 Agencies	Le 17 novembre 2020 Destinataires : Propriétaires d'infrastructures essentielles du Nouveau-Brunswick, Organisation des mesures d'urgence du Nouveau-Brunswick Services de police, d'incendie et d'ambulance et responsables des services 911 du Nouveau-Brunswick
CRITICAL INFRASTRUCTURE ALERT **Event Description** As a follow up to the Cyber CI Alerts sent over the weekend of November 14th, please see attached for additional Indicators of Compromise (IOC's) from an active cyber threat within the province of New Brunswick. Furthermore, a second document has been attached describing the H.A.L.T technique, designed to help teach the skills required to better recognize phising emails. **RECOMMENDED ACTIONS** We strongly recommend that this information be forwarded to your IT department so they can check network and firewall logs against these IOC's, block potential threats, and adjust SIEM and other detection systems to alert on these IOCs. Also, check for recently created network and e-mail accounts with elevated privileges. OPSA also suggests wide distribution of the H.A.L.T technique document to employees within your organization for educational purposes in order to strengthen the security of your organization. OPSA will continue to monitor the situation and receive updates from its federal, provincial,	**ALERTE SUR LES INFRASTRUCTURES ESSENTIELLES** **Description de l'événement** Pour donner suite aux alertes sur les infrastructures essentielles publiées pendant la fin de semaine du 14 novembre, vous trouverez ci-joint d'autres indicateurs de compromission d'une cybermenace active présente au Nouveau-Brunswick. Nous vous transmettons également un document décrivant la technique G.A.R.E. conçue pour apprendre à reconnaître les courriels hameçons. **MESURES RECOMMANDÉES** Nous vous recommandons fortement d'acheminer cette information à votre service des technologies de l'information afin qu'il puisse vérifier votre réseau et les registres sur les pares-feux, bloquer toute possibilité de menace et ajuster votre système de gestion des informations et des événements de sécurité et autres systèmes de détection en fonction de ces indicateurs de compromission. Ils doivent également vérifier si de nouveaux réseaux et comptes de courriel avec privilèges étendus ont été créés récemment. Le BCPS recommande aussi de distribuer aux membres du personnel le document sur la technique G.A.R.E. afin de les sensibiliser au phénomène d'hameçonnage et de renforcer la sécurité de votre organisation.

territorial, and municipal partners. Should the situation change, OPSA will update you in a timely manner. If you have questions or concerns, please contact the Office of the Provincial Security Advisor at (506) 457-7535.	Le BCPS continuera à surveiller la situation et recevra des mises à jour de ses partenaires fédéral, provinciaux, territoriaux et municipaux. Si la situation évolue, le BCPS vous informera dans les plus brefs délais. Si vous avez des questions, veuillez communiquer avec le Bureau du conseiller provincial en matière de sécurité du ministère de la Sécurité publique du Nouveau-Brunswick au 506-457-7535.
Critical Infrastructure (CI) Communications Scale **CI Information Note:** Critical Infrastructure Information Notes are messages designed to increase awareness of a specific topic and do not imply any change in the level of threat or risk. **CI Advisory:** Advisories are used to communicate information about potential, imminent or actual threats, vulnerabilities or incidents assessed as limited in scope but having possible impact on critical infrastructure. **CI Alert:** Alerts are used to communicate information about potential, imminent or actual threats, vulnerabilities or incidents where precautions and actions are required.	**Échelle de communication sur les infrastructures essentielles** **Note d'information sur les infrastructures essentielles :** Les notes d'information sur les infrastructures essentielles sont des messages envoyés à titre informatif sur un sujet en particulier et n'indiquent pas des changements au niveau de la menace ou du risque. **Avis sur les infrastructures essentielles :** Les avis sont émis pour communiquer des renseignements au sujet de menaces possibles, imminentes ou réelles, de vulnérabilités ou d'incidents que l'on estime limités en portée, mais pouvant avoir des répercussions sur les infrastructures essentielles. **Alerte sur les infrastructures essentielles :** Les alertes sont utilisées pour communiquer des renseignements sur les menaces possibles, imminentes ou réelles, les vulnérabilités ou les incidents, ainsi que sur les précautions et les mesures qui doivent être prises.