Perimeter Security and Economic Competitiveness

Sécurité du périmètre et compétitivité économique

Cybersecurity Action Plan

Between Public Safety Canada and the Department of Homeland Security

Public Safety Canada

Sécurité publique Canada

U.S. Department of Homeland Security

CYBERSECURITY ACTION PLAN
BETWEEN PUBLIC SAFETY CANADA
AND THE DEPARTMENT OF HOMELAND SECURITY

INTRODUCTION

Public Safety (PS) Canada and the Department of Homeland Security (DHS) are pursuing a coordinated approach to enhance the resiliency of our cyber infrastructure. The Cybersecurity Action Plan (the Action Plan) between PS and DHS seeks to enhance the cybersecurity of our nations through increased integration of PS' and DHS' respective national cybersecurity activities and improved collaboration with the private sector. This Action Plan represents just one of many important efforts between Canada and the United States to deepen our already strong bilateral cybersecurity cooperation.

As the Internet knows no borders, all countries have a responsibility to prevent, respond to, and recover from cyber disruptions and to make cyberspace safer for all citizens across the globe. Due to a shared physical border, Canada and the United States have an additional mutual interest in partnering to protect our shared infrastructure. This Action Plan aims to articulate a shared approach to fulfill PS' and DHS' vision of working together to defend and protect our use of cyberspace and to strengthen the resiliency of our nations. These efforts, combined, advance the objectives articulated by President Obama and Prime Minister Harper in the February 2011 declaration, *Beyond the Border: A Vision for Perimeter Security and Economic Competitiveness*.

This Action Plan outlines three goals for improved engagement, collaboration, and information sharing at the operational and strategic levels, with the private sector, and in public awareness activities, for activities conducted by PS and DHS. The Action Plan establishes lines of communication and areas for collaborative work critical to enhancing the cybersecurity preparedness of both nations. The Action Plan's goals and objectives are to be conducted in accordance with the June 2012 *Statement of Privacy Principles by the United States and Canada*. This Action Plan is intended to remain a living document to be reviewed on a regular basis and updated as needed to support new requirements that align to the Plan's key goals and objectives. It intends to support and inform current and future efforts to advance the goals of *Beyond the Border*, which ultimately seeks to enhance broad bilateral cooperation on cybersecurity efforts across both governments.

GOALS AND OBJECTIVES

1. Enhanced Cyber Incident Management Collaboration between National Cybersecurity Operations Centers

PS' Canadian Cyber Incident Response Centre intends to work jointly with DHS' United States Computer Emergency Readiness Team and Industrial Control Systems Cyber Emergency Response Team towards the following objectives:

1.1 Increase real-time collaboration between analysts by improving existing channels for remote communication and arranging in-person visits;

1.2 Enhance information sharing at all classification levels and collaborate on training opportunities, while promoting inter-agency coordination, as appropriate, as well as the proper protections for information, as outlined in the *Statement of Privacy Principles*;

1.3 Coordinate on cybersecurity incident response management, relating to defense, mitigation, and remediation activities and products, including with other public and private entities consistent with each country's laws and policies;

1.4 Align and standardize cyber incident management processes and escalation procedures; and

1.5 Enhance technical and operational information sharing in the area of industrial control systems security.

2. Joint Engagement and Information Sharing with the Private Sector on Cybersecurity

Due to the shared nature of critical infrastructure between Canada and the United States, PS and DHS intend to collaborate on cybersecurity-focused private-sector engagement for cybersecurity activities for which they are responsible through the following objectives:

2.1 Share engagement approaches for private sector;

2.2 Exchange and collaborate on the development of briefing materials for the private sector;

2.3 Jointly conduct private sector briefings;

2.4 Review approaches and align processes for private sector engagement through requests for technical assistance and non-disclosure agreements; and

2.5 Standardize protocols for sharing information.

3. Continued Cooperation on Ongoing Cybersecurity Public Awareness Efforts

Cybersecurity is a shared responsibility and everyone, including our citizens, has a role to play. With increased media attention devoted to cybersecurity incidents and with the continuing growth of electronic commerce and social media, it is imperative that citizens receive clear and trustworthy information on how to manage cyber threats to themselves and their families. Ensuring that government's cybersecurity awareness messages are consistent across our border helps to deliver that information effectively and consistently. PS Communications, the DHS Office of Public Affairs, and the National Protection and Program Directorate's Office of Cybersecurity and Communications (CS&C) intend to continue to work together as they:

3.1 Collaborate on public awareness campaigns (websites, social media activities, education material, etc.);

3.2 Collaborate on Cybersecurity Awareness Month (October); and

3.3 Share and coordinate messaging on issues of common interest.

GOVERNANCE OF THE JOINT ACTION PLAN

Senior officials within PS and CS&C intend to review and provide additional guidance in order to update this Action Plan on a quarterly basis. This Action Plan is intended to be a part of broader inter-governmental coordination across government agencies in both the United States and Canada.