ITS Products Pre-Qualification Program

Ghislain Lagacé

Designated Cryptographic Systems Program Manager

Communications Security Establishment

AIM

To provide an overview of the CSE ITS Product Pre-qualification Program (IPPP)

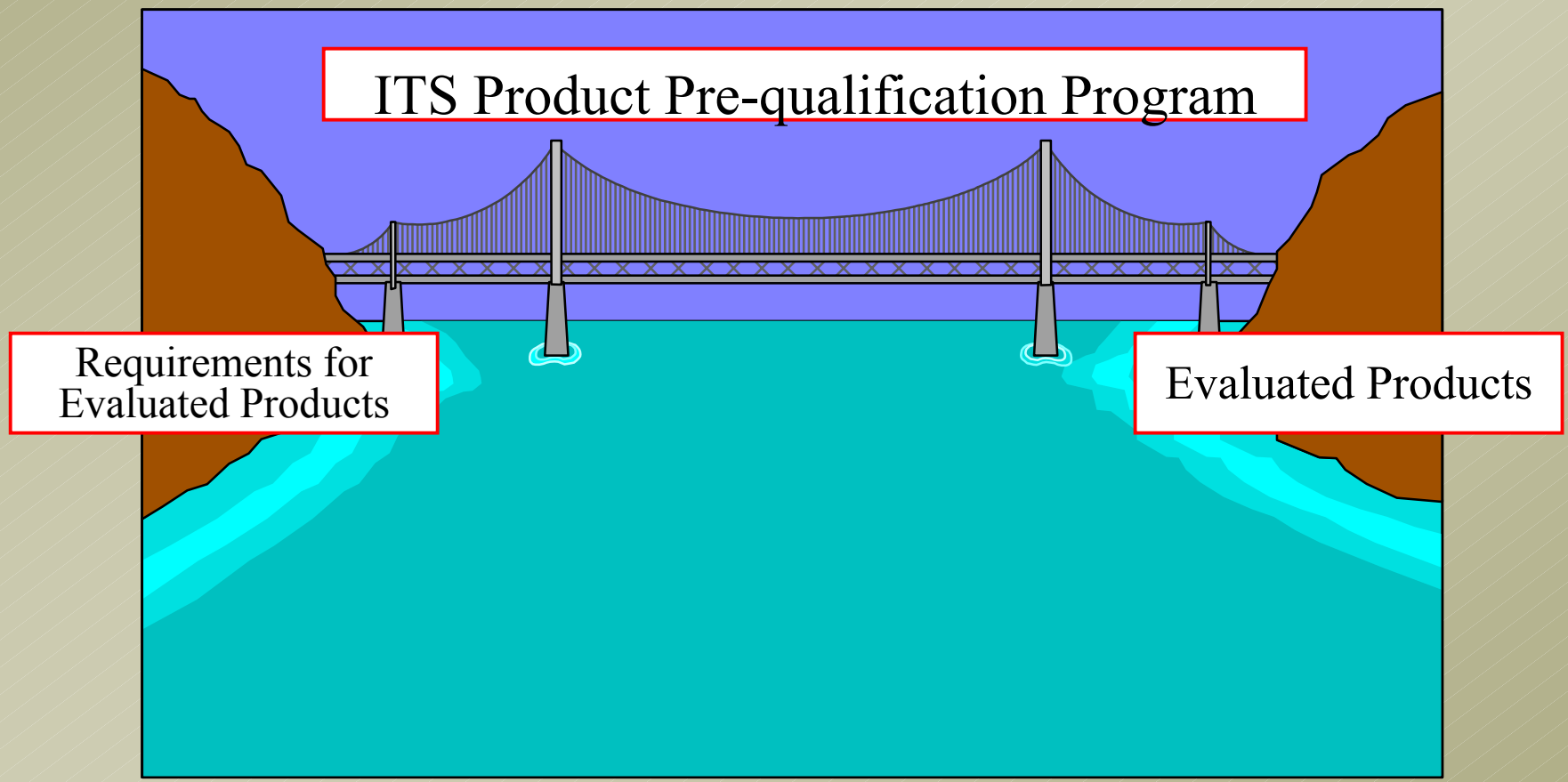
Applicability of FIPS 140-1

- In Canada, use of validated crypto modules is not mandatory for low sensitive information
- CSE encourages Canadian federal departments to use validated crypto modules and approved algorithms
- Interest is constantly increasing in government

The “Gap”

- Procurement process mainly driven by cost
- Evaluated ITS products are mostly treated the same as unevaluated products
- Potential of procuring unevaluated ITS products with unknown risks
- Government wants easier access to evaluated ITS products

Bridging the “Gap”



ITS Product Pre-qualification Program (IPPP)

- Objective of the Program is to facilitate the procurement of pre-qualified ITS products that meet or exceed a minimum level of assurance for the protection of GoC sensitive information

Program Overview

- Procurement tool for pre-qualified ITS products
- Jointly managed by CSE and PWGSC
- Program doesn't overrule PWGSC procurement rules
- Product must have been analyzed under one of the Component Programs and deemed suitable
- Provides a list of ITS products that meet CSE's criteria from which Government departments can choose from

Component Programs

- Cryptographic Module Validation Program (FIPS 140-1 & 140-2)
- Common Criteria Scheme
- Cryptographic Endorsement Program
- "Examination" of products that use or incorporate a validated crypto module

IPPP is Independent of the Component Programs

IPPP Pre-qualification Requirement

- Product validated to FIPS 140-1/2 or integrates a crypto module validated to FIPS 140-1/2 under the CMVP and uses CSE approved cryptographic algorithms
- Certified under Common Criteria Scheme
- Undergo an examination process by CSE

Examination Process

- Product must:
  - use or integrate a validated cryptographic module
  - use CSE approved cryptographic algorithms
- Program analyses:
  - the implementation of the validated crypto module
  - implementation of the approved algorithms
- Focus on CRYPTO features, not COMPUSEC features
- 2 - 3 day effort
- *Products* are pre-qualified at “examined” version

ITS Product Pre-qualification Program

Cryptographic Security

- CMVP
  - Products validated to FIPS 140-1
  - Products that incorporate or use validated crypto modules
  - Must use CSE approved cryptographic algorithms
- CEP

Computer Security

- Canadian Common Criteria Scheme Products evaluated or recognized by the Canadian Common Criteria Scheme

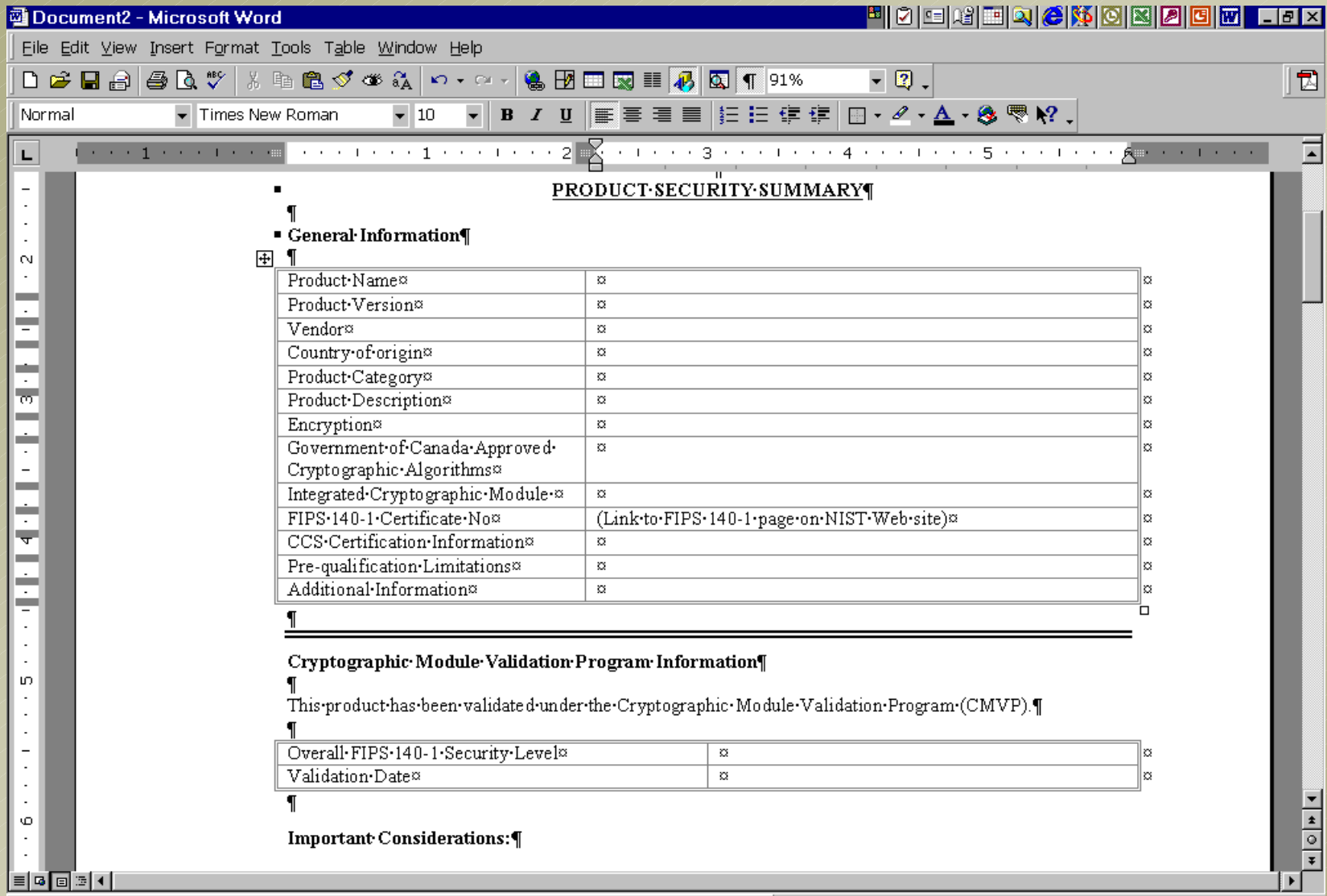
ITS Pre-qualified Product List

ITS Pre-qualified Product List

- Program output

  www.cse-cst.gc.ca/en/services/industrial_services/its_pre-qual_prod_list.html
- Contains the list of pre-qualified ITS products used for procurement by PWGSC
- Divided into product categories for ease of use
- Product Security Summary sheets

In time, ITS products on the list will be the preferred ones for procurement


Document2 - Microsoft Word
File Edit View Insert Format Tools Table Window Help
Normal
Times New Roman
10
91%
PRODUCT SECURITY SUMMARY
General Information
Product Name
Product Version
Vendor
Country of origin
Product Category
Product Description
Encryption
Government of Canada Approved Cryptographic Algorithms
Integrated Cryptographic Module
FIPS 140-1 Certificate No
(Link to FIPS 140-1 page on NIST Web site)
CCS Certification Information
Pre-qualification Limitations
Additional Information
Cryptographic Module Validation Program Information
This product has been validated under the Cryptographic Module Validation Program (CMVP).
Overall FIPS 140-1 Security Level
Validation Date
Important Considerations:
Draw
AutoShapes
Page 1 Sec 1 1/3 At 4.9" Ln 21 Col 1 REC TRK EXT OVR English (Cana
Start
Exploring - Ippl
ITS Pre-qualified Pr...
Microsoft PowerPoi...
Document1 - Micros...
Document2 - Mic...
10:44 AM

How to get pre-qualified?

- Vendor must request CSE to pre-qualify their product
- CMVP
  - Provide validation certificate number
- CCS
  - Provide CC documentation

    (Security Target; Certification Report; Evaluation Technical Report)

How to get pre-qualified?

- Provide general corporate information
- "Examination" of product using or incorporating validated crypto modules
  - Provide product and product information
  - CSE examine the product to confirm use of claimed cryptographic module.

Advantages to industry

- CSE confirmation that item meets the claimed security standard
- No need to convince potential clients that the product is fit for purpose
- Product visibility to other levels of government, industry and citizens
- Potential savings in sales and marketing costs
- Potential return on investment for evaluation

Advantages to Government

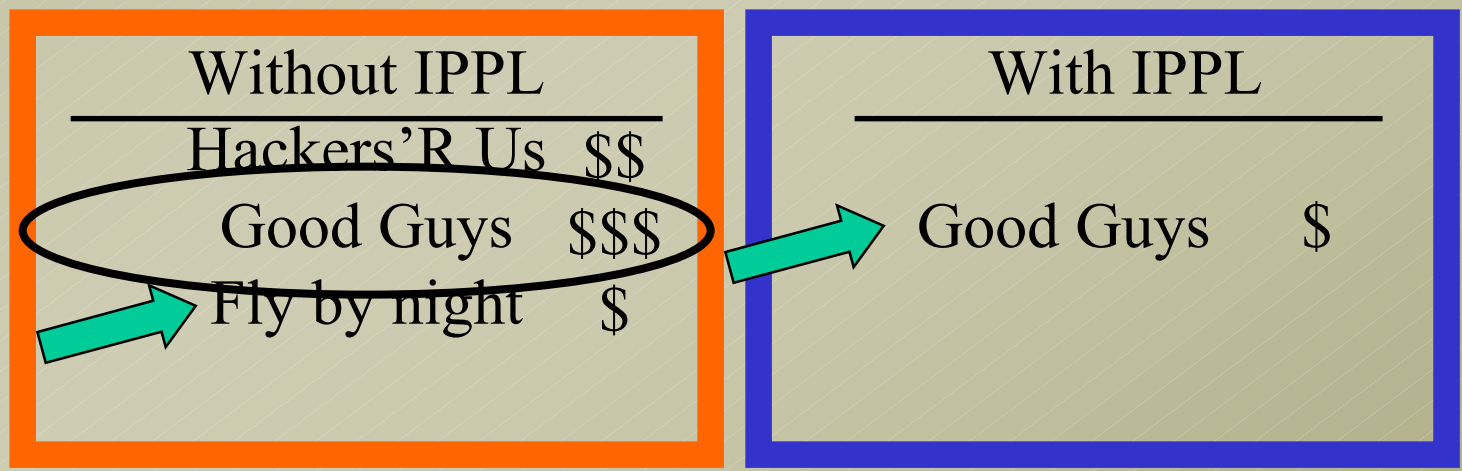
- CSE confirmation that item performs as advertised
- No need to conduct separate evaluations
- Potential savings in time and resources
- All products on one list

Procurement Process with IPPP

- Normal tendering process applies
- Requirement specifications
  - Complete technical requirement specs
  - Must also specify product pre-qualification
- PWGSC publishes an ACAN or NPP, and invites vendors with pre-qualified products to submit offers

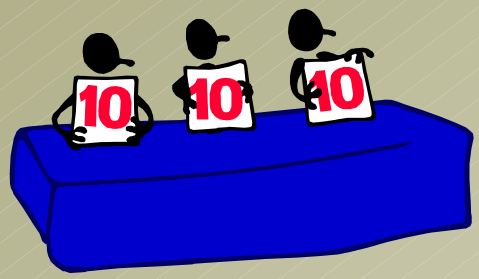
ACAN Process
(Sole source)

ACAN is published on GETS when only one product meets specifications AND is pre-qualified



NPP Process
(Multiple pre-qualified vendors)

- NPP is published on GETS when several products meet specifications AND are pre-qualified
- Source list is established
- RFP is issued only to companies whose products are pre-qualified



Win! – Win!

- Government Wins!
  - Greater level of assurance
  - Easier procurement process
- Vendor Wins!
  - Product differentiation and possible increased sell to government
  - Increased exposure to other government levels and industry

Vendors with pre-qualified products

- Alcatel
- Certicom Corp.
- Chrysalis-ITS
- Cisco Systems, Inc.
- Entrust Inc.
- E-Witness, Inc.
- Kasten Chase Applied Research Inc.
- L-3 Communications
- McAfee.com Corp. (Signal9 Solutions)
- nCipher Corporation Ltd
- Nortel Networks Ltd
- Preclarus
- Rainbow Technologies
- Research in Motion Ltd
- SecureLogix Corp.
- Spyrus
- Thales e-Security Ltd (Zaxus)
- ViaSafe, Inc.
- WinMagic, Inc.

CSE Website URLs

- CSE website
  - www.cse-cst.gc.ca
- Government Electronic Tendering System
  - www.merx.cebra.com
  - PW-$$QC-006-2005 to view LOI
- IPPL
  - www.cse-cst.gc.ca/en/services/industrial_services/its_prod_pre-qual_prog.html

Ghislain Lagacé

Designated Cryptographic Systems Program Manager

Communications Security Establishment

Ghislain.Lagace@cse-cst.gc.ca

(613) 991-8497