Security and Stability Update

18 November 2013

ICANN Global Domains Division

John Crain
Chief Security, Stability and
Resiliency Officer

ICANN 48 • 17-21 Nov 2013
Buenos Aires

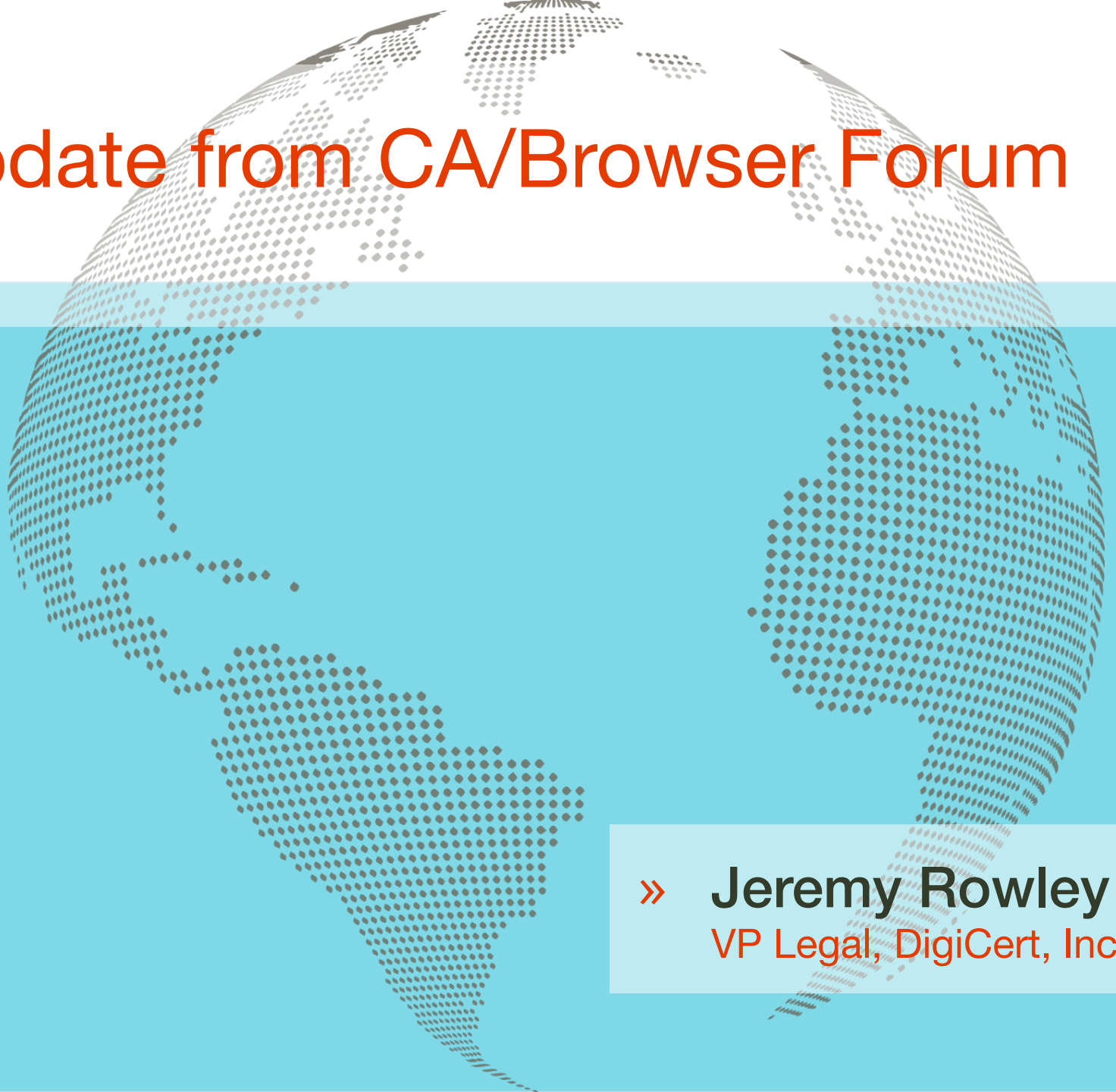
ICANN

ICANN @15

Agenda

- Update from CA/Browser Forum
- New gTLD Collision Occurrence Management Plan
- Name Collision Occurrence Management Framework
- Name Collision Identification and Mitigation for IT Professionals
- TLD Security Stability Management Risk and Incident Escalation Process

Update from CA/Browser Forum



» **Jeremy Rowley**
VP Legal, DigiCert, Inc.

CA/Browser Forum

Jeremy Rowley
DigiCert

CA/Browser Forum

Goal:

Improve the standard for online security by raising the bar on digital certificate and CA practices.

Membership:

- CAs
- Browsers
- Interested Parties (non-voting)

Standards:

- Baseline Requirements
- EV Guidelines
- Network Security Guidelines
- EV Code Signing Guidelines
- Code Signing Baseline Requirements

Developments

- Technology Changes
  - 1024 bit deprecation
  - SHA2 requirement
  - Internal name phase out
  - SSL beyond logins and shopping carts
  - OCSP stapling

- Implementations
  - CAA deployment
  - CT deployment
  - 120 day rule

Projects

- EV certificate expansion
  - Expand scope
  - Update for changing business practices
  - Focus on international
- Performance working group
  - Faster performance
  - Smaller certificates
  - Impact of technology
  - Best practices profile
- Code signing baseline standards
  - New requirements
- Certificate lifecycles

The Path Ahead

Improved Online Security

- New technologies
- Better standards & enforcement

Bumps in the Road

- Legacy devices/software
- Old paradigms
- Chicken vs. Egg

Transparency, Accountability & Self-Selection

- More visibility into certificate issuance
- Enhanced information

Questions?

Contact me:

Jeremy.rowley@digicert.com

Resources:

- https://www.cabforum.org/
- https://casecurity.org/

New gTLD Collision Occurrence Management Plan

» Francisco Arias
Director, Technical Services

Background

+ Between November 2012 and March 2013 ICANN was made aware of the potential name collision issues
+ 5 August 2013, first proposal for managing new gTLD collisions for public comment
+ 7 October 2013, Board NGPC adopted the New gTLD Collision Occurrence Management Plan

High-Risk Strings

- Strings “home” and “corp” are identified as high risk
- ICANN will defer delegating home and corp indefinitely
- ICANN will collaborate with technical and security communities to continue to study the issues presented by these strings

Outreach Campaign

- Make the public as well as private network operators aware of the possibility of name collision occurrences as new TLDs are delegated
- Advise users and private network operators of the measures that ICANN and new TLD registries are able to and will take to minimize the potential for unintended consequences or harm
- Assist users, private network operators, and software or equipment manufacturers with the identification of causes (origins) of name collisions.
- ICANN will collaborate with other parties and members of the community

120-Day No-Activation Period

+ Mitigates the Internal Name Certificate issue identified in SAC 057
+ Wait-period of no less than 120 days from registry agreement signed with no activation of names under the applied-for TLD in the DNS
+ The period is per CAs requirement to revoke certificates for new TLDs
+ Impact on TLD launch will be minimal

Name Collision Response

+ Last-resort response mechanism
+ Allows affected parties to report demonstrably severe harm as a consequence of name collision occurrences
+ ICANN central point to report issues at http://www.icann.org/en/help/name-collision
+ A Registry will review a reported case and could temporarily deactivate a name

Options for the Applicant

Primary Path

+ Use the Name Collision Occurrence Assessment (result of applying the Framework)

Alternate Path (25 strings not eligible):

+ Block all the SLDs seen in DITL and other relevant data

Name Collision Occurrence Management Framework

+ To be developed in cooperation with community
+ Will include parameters and processes to assess both probability and severity of impact
+ Will specify a set of assessments and corresponding mitigation measures
+ Focused on second level domain name (SLD)
+ Assessment per TLD

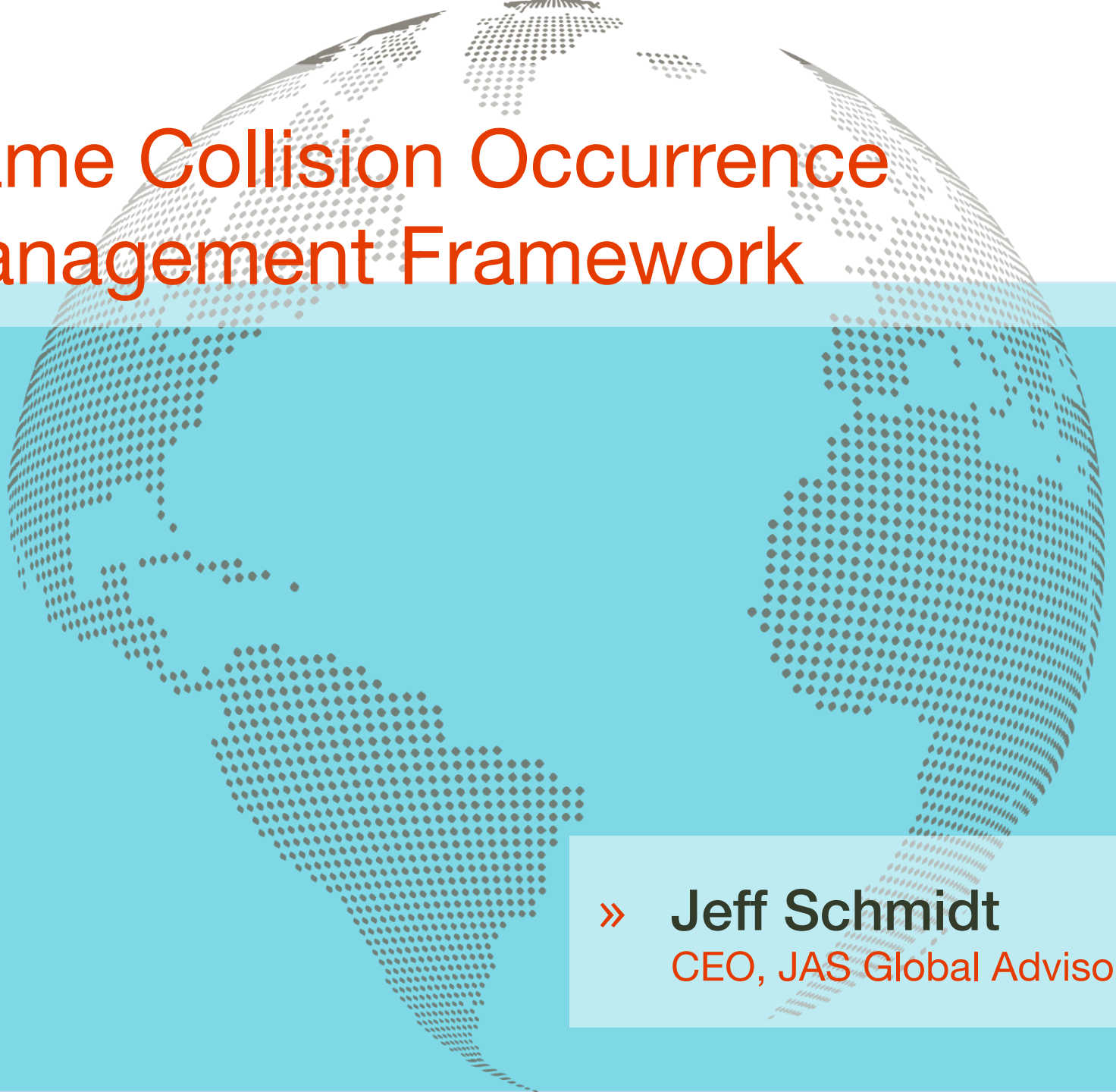
Alternate Path to Delegation

+ Conservative approach
+ Allows progress of the new gTLD Program without compromising security & stability
+ Temporary block all SLDs seen in 2006-2013 DITL datasets
+ Preserves DNS results (NXDOMAIN response) that the public DNS returns before delegating the TLD

Alternate Path to Delegation Eligibility

- Analysis showed that for 25 applied-for strings, the variance of SLDs queried is so significant that the mechanism of blocking SLDs might not be an effective way of addressing the name collision issue. This strings are ineligible to use the Alternate Path.
- For these strings, the year-over-year increase of the number of SLDs queried is an outlier as compared to the population of proposed gTLDs in:
  - at least one of the DITL samples 2006-2011, and
  - 2012 (indicates churn is currently occurring)

Name Collision Occurrence Management Framework



» **Jeff Schmidt**
CEO, JAS Global Advisors LLC

Where This Project Fits

ICANN has identified several phases of the broad DNS Name Collision Mitigation Strategy:

1. SLD Block List Strategy/Publication
2. Creation of the Name Collision Occurrence Management Framework
3. Applying the Framework to create per TLD Collision Occurrence Assessments

JAS has been engaged to complete (2)

High-level Objectives

- Timely
- Repeatable framework that will comprehensively address the name collision issue during introduction of new TLDs
- Applicable prior to or after TLD delegation
- Define paths for Registry Operators to remove strings from their block list
- Applied to create a specific Name Collision Occurrence Assessment for each applied-for TLD

Risk Assessment

+ Gain a better understanding of the potential consequences of collisions
+ The frequency of possible collisions has received substantial attention over the past several months; our primary objective is to advance discussion of the possible consequences from the theoretical to the concrete
+ Not all collisions are equal

Workstreams

+ Develop a taxonomy of queries and map to frequency data
+ Quantify the impact of malware/adware/ clickfraud tools
+ Analyze the effects of collisions in previous TLD delegations and within existing TLDs
+ Use Monte Carlo Analyses to understand the true probabilities of complex event chains

Workstreams (cont'd)

+ Compare risks associated with collisions to other technology risks
+ Use surveys and outreach to solicit feedback from the broader community
+ Develop Case Studies based on actual experiences with DNS name collisions
+ Develop specific options to manage risks

Specific Requests for Public Participation: Case Studies

+ We are interested in any relevant experience with DNS name collisions that may have occurred due to previous [g/cc] TLD delegations and within delegated TLDs
+ Will maintain anonymity and/or protect operational details as needed (including non-disclosure agreements)

Specific Requests for Public Participation: Information Concerning Algorithmic Queries

- The datasets are dominated by queries to labels that appear to be random/ algorithmically generated
- Certain sets of queries (such as the “Chrome 10” queries) are well understood but there are several other pervasive patterns:

[a-z0-9]{13} with exactly 1 '-’	c2gdAX7-upUzN
[a-z0-9]{13}	qgg75b8m2m70r
[a-z1-9:]{9}\.[0-9]{2}[a-z]{2}	yb9vxq65w.12hn
Microsoft GUID	6B29FC40-CA47-1067-B31D-00DD010662DA
_[0-9]{3}_[0-9]{2}_[0-9]	_891_43_6

Specific Requests for Public Participation: Survey

+ Solicit feedback from a broad community
+ Technical operations, business continuity, security, and risk management professionals
+ Encourage participation outside the ICANN Sphere

Specific Requests for Public Participation: Data

If you happen to have data:

+ Root
+ Large recursive
+ Authoritative for a delegated TLD

Please contact me (if I haven't already reached out!)

+ <namespacestudy@jasadvisors.com>

How to Stay Informed & Participate: DNS-OARC Collisions List

+ DNS-OARC Collisions List has been the unofficial epicenter for collisions-related discussion for the past several months
+ Interested parties should review the list archive and subscribe
+ JAS will continue to actively participate in discussions on this list
+ https://lists.dns-oarc.net/mailman/listinfo/collisions

How to Stay Informed & Participate:
Review the Technical Details

+ JAS actively maintains a page on the DNS-OARC site where technical details of our research, intermediate datasets, and pointers to our source code can be found
+ https://www.dns-oarc.net/node/332

How to Stay Informed & Participate: Provide Direct Feedback

+ Share ideas, commentary, and feedback with us directly
+ We may ask for permission to include some correspondence in our report
+ <namespacestudy@jasadvisors.com>

How to Stay Informed & Participate:
Review and Comment on the Draft Report

+ Expect a complete Draft report to be available in early January for an ICANN Public Comment Period
+ We will carefully consider all public comments and produce a final report thereafter
+ Final Name Collision Occurrence Management Framework is expected by the Singapore meeting in March 2014

How to Stay Informed & Participate:
Follow and Comment on DomainIncite

+ Members of the JAS Team will blog over the coming months concerning particular aspects of the project
+ Objective is to tighten feedback cycle and keep the information flowing

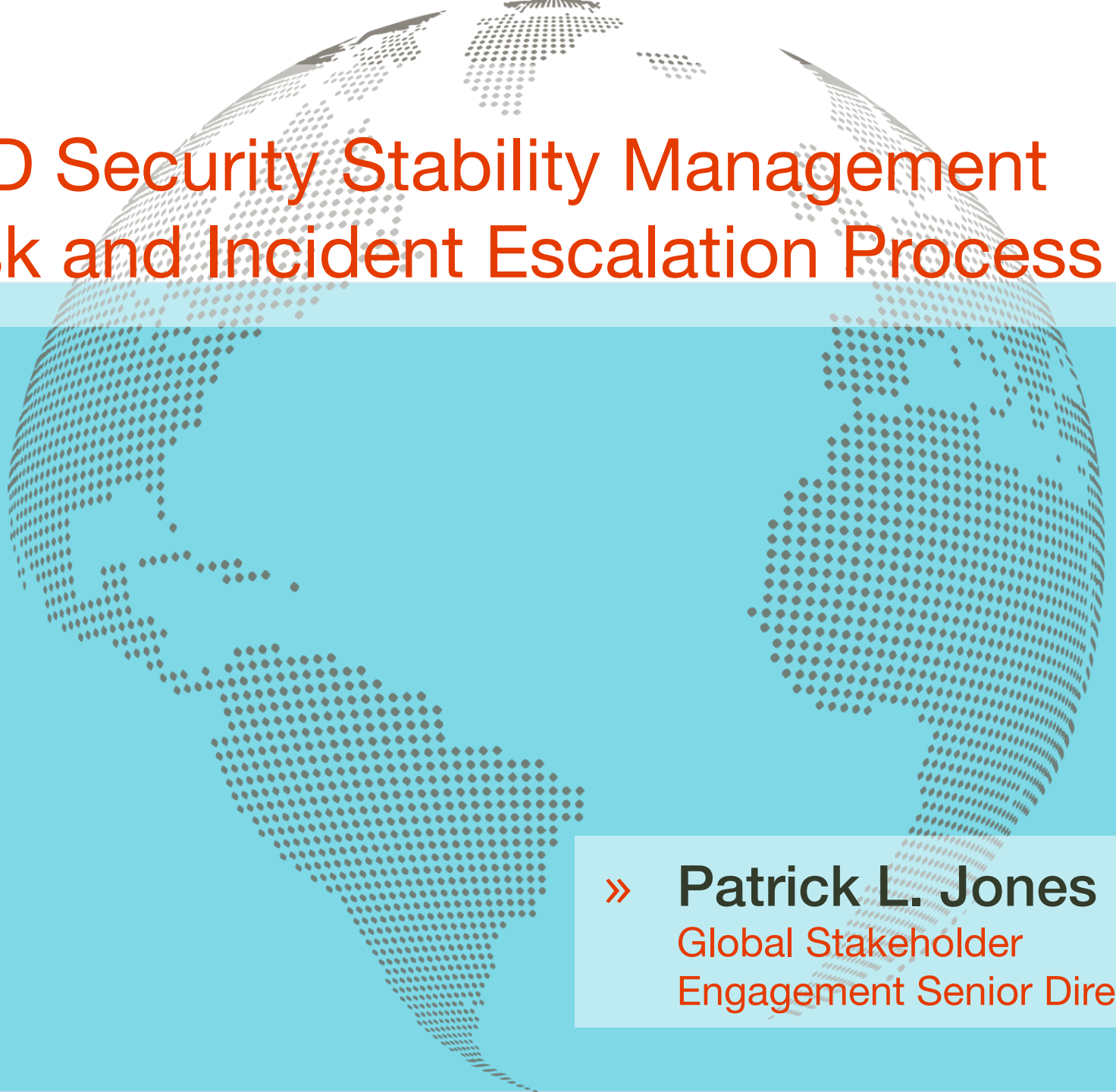
Name Collision Identification and Mitigation for IT Professionals

» **Dave Piscitello**
Vice President of Security
and ICT Coordination

Name Collision Identification and Mitigation for IT Professionals

- Describes problems that organizations may encounter when internal names leak to the global DNS if they are:
  - branching off of the global DNS
  - using their own roots with private TLDs
  - using search lists
- Recommended measures for mitigating these problems for private name spaces that

TLD Security Stability Management Risk and Incident Escalation Process



» **Patrick L. Jones**
Global Stakeholder
Engagement Senior Director

Questions?

Global Domains Division Sessions

Community Priority Evaluation & Auction

- Monday, 18 Nov 2013, 17:15-18:45; Libertador C

Contracting & Onboarding

- Wednesday, 20 Nov 2013, 10:30-12:00; Libertador C

Trademark Clearinghouse: Operations & Processes

- Wednesday, 20 Nov 2013, 15:30-16:30; Libertador C

IDN Variant TLDs Program

- Wednesday, 20 Nov 2013, 16:45-18:15; Libertador C

Continued Operations for new gTLDs

- Thursday, 21 Nov 2013, 11:00-12:30; Libertador AB