DSSA Report – Appendices

6. Appendices

6.1. Charter

Joint DNS Security and Stability Analysis Working Group (DSSA-WG)

Draft Charter

Version 1.0

12 November 2010

1.0 Background

At their meetings during the ICANN Brussels meeting the At-Large Advisory Committee (ALAC), the Country Code Names Supporting Organization (ccNSO), the Generic Names Supporting Organization (GNSO), the Governmental Advisory Committee (GAC), and the Number Resource Organization (NROs) acknowledged the need for a better understanding of the security and stability of the global domain name system (DNS). This is considered to be of common interest to the participating Supporting Organisations (SOs), Advisory Committees (ACs) and others, and should be preferably undertaken in a collaborative effort.

To this end the ALAC, ccNSO, GNSO and NRO agreed to establish a Joint DNS Security and Stability Analysis Working Group (DSSA-WG), in accordance with each own rules and procedures and invite other AC's to liaise and engage with the DSSA-WG in a manner they consider to be appropriate.

2.0 Objectives, Scope of Activities, and Deliverables

2.1 Objectives and Goals

The objective of the DSSA-WG is to draw upon the collective expertise of the participating SOs and ACs, solicit expert input and advice and report to the respective participating SOs and ACs on:

A. The actual level, frequency and severity of threats to the DNS;
B. The current efforts and activities to mitigate these threats to the DNS; and

C. The gaps (if any) in the current security response to DNS issues.

If considered feasible and appropriate, the DSSA-WG may identify and report on possible additional risk mitigation activities that it believes would assist in closing any gaps identified under item C above.

Each of the participating SOs and ACs has adopted this charter according to its own rules and procedures.

2.2 Scope of Activities

The DSSA-WG should limit its activities to considering issues at the root and top level domains within the framework of ICANN's coordinating role in managing Internet naming and numbering resources as stated in its Mission in its Bylaws. The DSSA-WG also should take into account and attempt to coordinate with existing, ongoing, and emerging research, studies, and initiatives with respect to the DSSA-WG objectives. Subject to the limitations above, the DSSA-WG should do whatever it deems relevant and necessary to achieve its objectives.

The DSSA-WG shall take a proactive role in fostering participation and input from the relevant communities and expert groups and provide regular feedback and the opportunity to comment to the participating SOs and ACs and the ICANN community in general on its progress. All DSSA-WG members are encouraged to keep their respective groups updated and to solicit feedback and provide that feedback to the DSSA-WG.

If issues become apparent to the DSSA-WG that are outside of its scope, the DSSA-WG Co-Chairs shall inform the Chairs of the participating SOs and ACs in a timely manner so that appropriate action or remediation can be taken.

2.3 Deliverables and Timeframes

2.3.1 Work Plan

As a first step the DSSA-WG shall establish and adopt a work plan and associated schedule. The Co-Chairs of the DSSA-WG shall inform the Chairs of the participating SOs and ACs accordingly. The Work Plan and schedule should include times and methods for public consultation and reporting to the participating SOs and ACs, including an expected date for submission of a Final Report. The tentative schedule included in Annex A, will be updated accordingly.

2.3.2 Reporting

The Co-Chairs of the DSSA-WG shall report regularly to the participating SOs and ACs on the progress of the DSSA-WG and at an appropriate time produce a Final Report on its findings with respect to items 2.1 A, B and C above.

2.4 Final Report

Following its submission each of the SOs and ACs shall discuss the Final Report and may adopt the Final Report according to their own rules and procedures. The Chairs of the SOs and ACs shall inform the Co-Chairs of the DSSA-WG accordingly within [one month, other term] after submission of the report.

3.0 Members, Staffing, and Organization

3.1 Membership

Membership in the DSSA-WG is open to members of the participating ICANN SOs and ACs. Each of the participating SOs and ACs shall appoint members to the DSSA-WG in accordance with their own rules and procedures. There shall be a minimum of one representative from each participating SO and AC.

Non-participating ICANN AC's are invited to appoint one or more liaisons according to their own rules and procedures.

The Chairs of the participating SOs and ACs, or their alternates, shall be ex-officio members of the DSSA-WG.

The ALAC, ccNSO, and the GNSO shall each select a Co-Chair for the DSSA-WG. The Co-Chairs shall have primary leadership responsibilities for the DSSA-WG. The Co-Chairs are encouraged to collaborate with one another and with ICANN staff support personnel in leading the DSSA-WG.

The DSSA-WG shall also approach the technical and security communities, other DNS experts and CERTS to seek their participation in the activities the WG. The Co-Chairs of the DSSA-WG, after consulting the DSSA-WG members, may invite or appoint members of these groups to the membership of the DSSA-WG.

All DSSA-WG participants are expected to be able to:

- Demonstrate knowledge or expertise of aspects of the objectives of the DSSA-WG; and

- Commit to actively participate in the activities of the working group on an ongoing and long-term basis.

Participants and liaisons will be listed on the working group's webpage.

3.2 *Access to and Protection of Confidential Information*

Sub-working groups of the DSSA-WG may need to access sensitive or proprietary information in order for the DSSA-WG to do its work. Thus, measures may need to be established to access and protect confidential or proprietary information. The following procedures are an exception to the standards for transparency and accountability and only apply in cases where members of the aforementioned sub-working groups of the DSSA-WG need to access and to protect confidential information:

- In certain cases under this exception, in order to ensure access to and protection of confidential or proprietary information, sub-working groups' members of the DSSA-WG will be asked to sign a Formal Affirmation of Confidentiality and Non-Disclosure (See Annex B). In addition, the sub-working groups' members of the DSSA-WG may be required to sign a Non-Disclosure Agreement (NDA) for a specific project or issue.
- No formal Non-Disclosure Agreement (NDA) is required for membership in the DSSA-WG; and
- A separate email distribution list that is not publicly accessible may be established only to include the sub-working groups' members who have signed a Non-Disclosure Agreement applicable to that specific project or issue.

3.3 Statements of Interest (SOI)

Members of the DSSA-WG shall provide to the participating SO and AC Secretariats a Statement of Interest according to the rules set forth in the GNSO Council Operating Procedures at: http://gnso.icann.org/council/gnso-op-procedures-05aug10-en.pdf . SoI's shall be posted on the DSSA-WG website.

Pending revisions to section 5.3.3 of the GNSO Operating Procedures relating to Statements of Interest, members of the DSSA-WG shall provide the following information in their Statements of Interest:

1. Current vocation, employer and position
2. Type of work performed in #1 above
3. Identify any financial ownership or senior management/leadership interest in that are interested parties in DSSA related topics.
4. Identify any type of commercial or non-commercial interest in DSSA related topics. Are you representing other parties? Describe any arrangements/agreements between you and any other group, constituency or person(s) regarding your nomination/selection as a work team member.
5. As referenced in Section 3.1 above, DSSA-WG members are expected to "demonstrate knowledge or expertise of aspects of the objectives of the DSSA-WG". Please identify any knowledge, expertise or experience you have that would be relevant to the work of the DSSA-WG.
6. Describe any tangible or intangible benefit that you receive from participation in such processes. For example, if you are an academic or NGO and use your position to advance your ability to participate, this should be a part of the statement of interest, just as should employment by an organization that has an interest in DSSA WG outcomes.

3.4 Support staff and Tools

ICANN is expected to provide adequate staff support to the DSSA-WG.

In addition, the following communication tools have been established to aid the work of the DSSA-WG:

- DSSA-WG Wiki Workspace at (URL TBD)
- DSSA-WG Email List Subscriptions (TBD); and
- DSSA-WG SOI Repository at (URL TBD)

3.5 Rules of Engagement

The Co-Chairs, in consultation with participating SOs and ACs, are empowered to restrict the participation of someone who seriously disrupts the DSSA-WG. Any such restriction shall be reviewed by the participating SOs and ACs. Generally, the participant should first be warned privately, and then warned publicly before such a restriction is put into place. In extreme circumstances, this requirement may be bypassed. This restriction is subject to the right of appeal as outlined below.

3.6 Working Group Methodology

3.6.1 Standard Methodology for Making Decisions

In considering its work plan and reports the DSSA-WG shall seek to act by consensus. If a minority opposes a consensus position, that minority position shall be incorporated in the related report. The consensus view of the DSSA-WG members and minority views, if any, shall be conveyed to the participating SO's/AC's according to the following procedures.

The Co-Chairs shall be responsible for designating each position as having one of the following designations:

- Full consensus – a position where no minority disagrees;
- Consensus - a position where a small minority disagrees but most agree;
- No consensus but strong support for a specific position / recommendation but significant opposition; and
- Divergence – no strong support for a specific position / recommendation

In the case of consensus, no consensus or divergence, the DSSA-WG Co-Chairs should encourage the submission of minority viewpoint(s).

Based upon the DSSA-WG's needs and/or the Co-Chairs' direction, DSSA-WG participants may request that their names are not associated explicitly with any view/position.

If a participating SO or AC wishes to deviate from the standard methodology for making decisions or empower the DSSA-WG to use its own decision-making methodology it should be affirmatively stated in the DSSA-WG Charter.

Consensus calls should always make best efforts to involve the entire DSSA-WG. It is the role of the Co-Chairs to designate which level of consensus is reached and announce this designation to the DSSA-WG. Member(s) of the DSSA-WG should be able to challenge the designation of the Co-Chairs as part of the DSSA-WG discussion. However, if disagreement persists, members of the DSSA-WG may use the process described below to challenge the designation.

If any participant(s) in the DSSA-WG disagree with the designation given to a position by the Co-Chairs or any other consensus call, they may follow these steps sequentially:

1. Send email to the Co-Chairs, copying the DSSA-WG email list explaining why the decision is believed to be in error.
2. If the Co-Chairs still disagree with the complainants, the Co-Chairs shall forward the appeal to the SO and AC liaison(s). The Co-Chairs must explain their reasoning in the response to the complainants and in the submission to the liaison. If the SO and AC liaison(s) supports the Co-Chairs' position, the liaison(s) shall provide their response to the complainants. The liaison(s) must explain their reasoning in the response. If the SO and AC liaison(s) disagree(s)with the Co-Chairs, the liaison(s) shall forward the appeal to the participating SO and ACs. Should the complainants disagree with the liaison(s) support of the Co-Chairs' determination, the complainants may appeal to the Chairs of the SO or AC or their designated representatives. If the SO or AC agrees with the complainants' position, the SO or AC should recommend remedial action to the Co-Chairs.
3. In the event of any appeal, the SO or AC liaison(s) shall attach a statement of the appeal to the DSSA-WG report. This statement should include all of the documentation from all steps in the appeals process and should include a statement from the participating SOs and ACs.[1]

3.6.2 Appeal Process

Any DSSA-WG member that believes that his/her contributions are being systematically ignored or discounted or wants to appeal a decision of the DSSA-WG or the participating SO or AC should first discuss the circumstances with the DSSA-WG Co-Chairs. In the event that the matter cannot be resolved satisfactorily, the DSSA-WG member should request an opportunity to discuss the situation with the Chairs of the SOs or ACs or their designated representatives.

In addition, if any member of the DSSA-WG is of the opinion that someone is not performing their role according to the criteria outlined in section 4.1 of this document, the same appeals process may be invoked.

4. **Omission In or Unreasonable Impact of Charter**

[1] It should be noted that ICANN also has other conflict resolution mechanisms available that could be considered in case any of the parties are dissatisfied with the outcome of this process.

In the event this charter does not provide guidance and/or the impact of the charter is unreasonable for conducting the business of the DSSA-WG, the Co-Chairs of the DSSA-WG shall decide if they think charter needs to be modified.

In the event it is decided that the charter needs to be modified to address the omission or unreasonable impact, the Co-Chairs may propose to modify the charter. A modification shall only be effective after adoption of the adjusted charter by the participating SOs and ACs in accordance with their own rules and procedures.

5. Closure and Working Group Self-Assessment

The DSSA-WG shall be dissolved upon receipt of the notofication of the Chairs of the SOs and ACs as foreseen in section 2.4 above or as directed jointly by the participating SOs and ACs.

6.0 Charter Document History

This section records key changes to the DSSA-WG Charter that take place after the adoption of the Charter.

Annex A Schedule

Milestone Event	**Start Date**	**End Date**	**Deliverables**
Draft DSSA-WG Charter	TBD	TBD	Charter
Invite and Establish Working Group Co-Chairs and Members	TBD	TBD	Working Group Members & Co-Chairs
Adopt a Work Plan and Time Schedule	TBD	TBD	Work Plan and Time Schedule
Produce Draft Report	TBD	TBD	Draft Report
Public Comment Period on Draft Report	TBD	TBD	Public Comment
Final Report Submitted to SOs and ACs	TBD	TBD	Final Report

ANNEX B: AFFIRMATION OF CONFIDENTIALITY AND NON-DISCLOSURE

Joint DNS Security and Stability Analysis Working Group (DSSA-
Affirmation of Confidentiality and Non-Disclosure

I, _____________________________, a member of the ICANN Joint DNS Security and Stability Analysis Working Group (DSSA-WG), affirm my intention to conform to the following:

1. As a member of the DSSA-WG, I may be provided certain technical data or information that is commercially valuable and not generally known in its industry of principal use (collectively referred to as "Proprietary Information") pursuant to the DSSA-WG's performance of its tasks. I will use reasonable care to hold in confidence and not disclose any Proprietary Information disclosed to me. Written information provided to me as a member of the DSSA-WG shall be considered Proprietary Information only if such information is clearly marked with an appropriate stamp or legend as Proprietary Information. Non-written information shall be considered Proprietary Information only if the discloser of such information informs the DSSA-WG at the time of disclosure that the information being disclosed is of a proprietary nature.
2. I shall have no obligation of confidentiality with respect to information disclosed to me if:
    a. such information is, at the time of disclosure, in the public domain or such information thereafter becomes a part of the public domain without a breach of this Affirmation; or
    b. such information is known to the DSSA-WG at the time it is disclosed to me; or
    c. such information has independently developed by the DSSA-WG; or
    d. such information is received by the DSSA-WG from a third party who had a lawful right to disclose such information to it; or
    e. such information is allowed to be disclosed with the written approval of the disclosing party.
3. I understand that I may be requested to sign a non-disclosure agreement in order to access information to perform a study, research, or other DSSA-WG tasks. I understand that if I decline to sign any such agreement, I will also be declining participation in the task requiring the execution of the non-disclosure agreement.
4. My obligations under this Affirmation shall expire one (1) year after I am no longer a member of the DSSA-WG

Signature of DSSA-WG member:__________________________

Name of DSSA-WG member: _____________________________

Date: __________________________ Place: __________________________

6.2. Risk Scenarios

6.2.1. Risk Scenario – Gaps in Policy, Management and Leadership Lead to Splitting the Root

6.2.1.1. Examples

6.2.1.1.1. Nation-state blocking policy and configuration error.

In order to fulfill an IP infringement resolution, one nation-state requires all providers under its sovereignty to block access to a certain domain name and also all related resolved IP addresses. It happens that the country also hosts some authoritative servers. Unfortunately due to the wording in the resolution the authoritative-DNS hosting provider makes an error while changing configuration files on the authoritative server while fulfilling its obligations under the resolution. This change also causes problems in the resolution of the address for users from other countries

6.2.1.1.2. Nation-state alternate root, cyber terrorism and DNS hacking.

A country or a certain number of countries develop their own internal domain system and isolates itself from the rest of the Internet. The same actors are behind a well known cyber terroristic group. Due to the fact that they do no belong to the root servers system anymore, the need of an operable Internet is not required for them anymore. The geopolitical group acquires a 0day regarding an undisclosed vulnerability of the DNS on the black market (the same scenario can be applied also to DNSSEC) and deploys it in retaliation after an international security organization resolution. The vulnerability has a domino effect: affecting not only the authoritative but also the recursive servers and disrupting the resolution all around the world. Since there is no central incident response coordination and due to the fact the malfunctions propagates with different timings the problem has major impacts to the Internet at a worldwide level.

6.2.1.1.3. US National Information Protection Plan (NIPP) -- "Policy, Governance, and Knowledge Failures" alternate-root scenario

The Internet is an open and global system, providing individuals and organizations a variety of opportunities for attacking the DNS infrastructure. Actors attack the infrastructure for various motivations and objectives. An incident that originates from a nation-state may be motivated by a desire for political influence or to achieve military objectives. In contrast, an incident from an individual or a small group may only be a manifestation of their desire to exercise control over a key part of the Internet infrastructure or to demonstrate their technical prowess. Policy, governance, and knowledge failures could cause significant economic and national security impacts to the DNS critical function, and they could result in political and diplomatic tensions between nation-state threat actors. An attacker could try to establish an alternate Internet root, to which

DNS inquiries could be diverted, instead of being directed to the "real" DNS root. The establishment of regional or alternative Internets could decrease interoperability and cause technical confusion. Such a situation could cause strategic consequences across multiple sectors. Internet market influences may not be strong enough to avoid the emergence of an alternate, authoritative root, if the political and strategic environment provides an opportunity to establish and manage an alternative root system.

6.2.1.2. Risk Factors to Analyze

6.2.1.2.1. Threat Sources

- Nation states
- Geo-political groups

6.2.1.2.2. Vulnerabilities

- External relationships/dependencies
- Inconsistent or incorrect decisions about relative priorities of core missions and business functions
- Infrastructure vulnerabilities
- Interventions from outside the process
- Lack of effective risk-management activities
- Mission/business processes (e.g., poorly defined processes, or processes that are not risk-aware)
- Poor inter-organizational communications

6.2.1.2.3. Predisposing Conditions that Reduce Risk

- Contractual relationships between entities
- Culture of collaboration built on personal trust relationships
- Diverse operational environments and approaches
- Diverse, distributed system architecture and deployment
- Mechanisms for providing (and receiving) risk assurances, and establishing trust-relationships, with external entities

6.2.1.2.4. Predisposing Conditions that Increase Risk

- Definitions of responsibility, accountability, authority between DNS providers
- Diverse operational environments and approaches
- Legal standing (and relative youth) of ICANN

6.2.1.2.5. Missing or Insufficient Security Controls

- Awareness and Training
- Incident Response
- Planning
- Program Management

- Risk Assessment

6.2.1.2.6. Threat Events

- Zone does not resolve or is not available
- Zone is incorrect or does not have integrity

6.2.1.2.7. Adverse Impacts

In the worst case there would be broad harm/consequence/impact to operations, assets, individuals, other organizations and the world if any of these threat-events occur. And in all cases there would be significant problems for registrants and users in the zone.

6.2.2. Risk Scenario – “Reductive” Forces (Security, Risk-mitigation, Control through rules, etc.) Lead to Splitting the Root

6.2.2.1. Examples

6.2.2.1.1. ISOC "Moats and Drawbridges" scenario.

Suggests the world of the Internet would be heavily centralized, dominated by a few big players with their own rules in “big-boys’ clubs.” Conflicts would be resolved through negotiation, not competition. Connections between networks would be the result of extensive negotiation and deal making. There would likely be strong regulation as governments seek to impose some public interest obligations and perhaps even controls on the equipment users can connect to the network. Much content would be proprietary and protected by strong intellectual property rights. Governments would control the behavior of networks and network users through legal mechanisms and sanctions. Barriers to entry would be high, with little incentive to expand networks beyond the largest and richest customers or regions. Innovation would be slow, only occurring when it would benefit the network owners. All players would have close political links to their mutual benefit.

6.2.2.1.2. ISOC "Boutique Networks" scenario.

Envisions a future in which political, regional and large enterprise interests fail to maximize the social and economic potential of a shared, global set of richly connected networks (the Internet). It carries the weight of self-interest brought by factions seeking to optimize control in small sectors (political and otherwise). It also suggests these fractionalized networks will continue to leverage the benefits of existing Internet standards and technology. Each proprietary provider draws as much as possible from the common pool while giving little back.

6.2.2.2. Risk Factors to Analyze

6.2.2.2.1. Threat Sources

- External parties and contractors -- large content and network providers
- International governance/regulatory bodies

6.2.2.2.2. Vulnerabilities

- External relationships/dependencies
- Inconsistent or incorrect decisions about relative priorities of core missions and business functions
- Interventions from outside the process
- Lack of effective risk-management activities

- Poor inter-organizational communications

6.2.2.2.3. Predisposing Conditions that Reduce Risk

- Culture of collaboration built on personal trust relationships
- Diverse operational environments and approaches
- Diverse, distributed system architecture and deployment
- Emphasis on resiliency and redundancy
- Multi-stakeholder, consensus-based decision-making model

6.2.2.2.4. Predisposing Conditions that Increase Risk

- Definitions of responsibility, accountability, authority between DNS providers
- Legal standing (and relative youth) of ICANN
- Managerial vs. operational vs. technical security skills/focus/resources

6.2.2.2.5. Missing or Insufficient Security Controls

- Awareness and Training
- Planning
- Program Management
- Risk Assessment

6.2.2.2.6. Threat Events

- Zone is incorrect or does not have integrity

6.2.2.2.7. Adverse Impacts

In the worst case there would be broad harm/consequence/impact to operations, assets, individuals, other organizations and the world if any of these threat-events occur. And in all cases there would be significant problems for registrants and users in the zone.

6.2.3. Risk Scenario – Impacts of Natural Disasters

6.2.3.1. Examples

Note: in this phase, both of the example risk-scenarios focused on power-outages when thinking about natural disasters. The DSSA may rework this a bit as it proceeds into the next phase of its work.

6.2.3.1.1. Wide-ranging power outage

Someone forgot to remove a grounding strap from a major transmission line before re-energizing it. The rest of the grid tries to compensate, leading to a long lasting, cascading failure of the entire North American power grid. Due to the caching and redundant nature of the DNS, and the fact that many operators have generators, nothing bad happens... initially. As sites run out of fuel, more and more major authoritative providers go dark. The DNS serving side is well replicated, but the provisioning side is not. Zone files begin to expire, many of these could be saved (by promoting backups to masters / bumping the serial numbers, etc.) but, while there is a good culture of collaboration between many members of the community, much of the communication / recovery work is hampered by employees not having access to their work machines, to their address books and not having power at home.

6.2.3.1.2. Power outage

Due to a major blackout in a really populated area that also hosts several global and local instances of the root servers, the domain name resolution fails. Due to the Time to Live expiration and the duration of the black out the other instances around the world are overwhelmed by the requests as they were under a non-adversarial DDOS attack.

6.2.3.2. Risk Factors to Analyze

6.2.3.2.1. Threat Sources

- Blackout/Energy Failure

6.2.3.2.2. Vulnerabilities

- Business continuity vulnerabilities
- Infrastructure vulnerabilities
- Lack of effective risk-management activities
- Poor inter-organizational communications

6.2.3.2.3. Predisposing Conditions that Reduce Risk

- Emphasis on resiliency and redundancy
- Diverse, distributed system architecture and deployment
- Diverse operational environments and approaches
- Culture of collaboration built on personal trust relationships

6.2.3.2.4. Predisposing Conditions that Increase Risk

Contractual relationships between entities

- Diverse operational environments and approaches

6.2.3.2.5. Missing or Insufficient Security Controls

- Awareness and Training
- Configuration Management
- Contingency Planning

- Contingency Planning

Physical and Environmental Protection

- Risk Assessment

6.2.3.2.6. Threat Events

- Zone does not resolve or is not available

6.2.3.2.7. Adverse Impacts

In the worst case there would be broad harm/consequence/impact to operations, assets, individuals, other organizations and the world if any of these threat-events occur. And in all cases there would be significant problems for registrants and users in the zone.

6.2.4. Risk Scenario – Attacks Exploiting Technical Vulnerabilities of the DNS

6.2.4.1. Examples

6.2.4.1.1. Global, massive attack against a day zero vulnerability in DNS software, sustained until remediation is implemented.

6.2.4.1.2. DDOS attack on root server(s) or .com

6.2.4.1.3. Disgruntled employee.

An employee has just been fired due to HR cut from a company that operates several critical DNS services. The employee was in charge of these critical services and his credentials haven't been revoked immediately. The employee was normally dealing with issues due to the replication of the zone file and decides to implement a change and let it propagate. Due to the company resizing and lack of backup knowledge, an immediate response to customers complains is not provided and a major top-level domain experiences several hours of outages.

6.2.4.2. Risk Factors to Analyze

6.2.4.2.1. Threat Sources

- Rogue elements
- Insiders

6.2.4.2.2. Vulnerabilities

Inadequate incident-response

- Inadequate training/awareness
- Infrastructure vulnerabilities
- Operational vulnerabilities
- Security architectures (e.g., poor architectural decisions resulting in lack of diversity or resiliency in organizational information systems)
- Technical vulnerabilities

6.2.4.2.3. Predisposing Conditions that Reduce Risk

- Contractual relationships between entities
- Diverse, distributed system architecture and deployment
- Diverse, distributed system architecture and deployment
- Emphasis on resiliency and redundancy
- Managerial vs operational vs technical security skills/focus/resources

6.2.4.2.4. Predisposing Conditions that Increase Risk

- Culture of collaboration built on personal trust relationships
- Diverse operational environments and approaches
- Mechanisms for providing (and receiving) risk assurances, and establishing trust-relationships, with external entities

6.2.4.2.5. Missing or Insufficient Security Controls

- Configuration Management
- Identification and Authentication
- Incident Response
- Operational Controls
- Security Assessment and Authorization
- System and Communications Protection

6.2.4.2.6. Threat Events

- Zone is incorrect or does not have integrity
- Zone does not resolve or is not available

6.2.4.2.7. Adverse Impacts

In the worst case there would be broad harm/consequence/impact to operations, assets, individuals, other organizations and the world if any of these threat-events occur. And in all cases there would be significant problems for registrants and users in the zone.

6.2.5. Risk Scenario – Inadvertent Technical Mishaps

6.2.5.1. Examples

6.2.5.1.1. Invalid Signature Files

An invalid signature on a zone file is created – due to a combination of DNSSEC production errors, hardware or software failures or administrative process failures. Either the root or a TLD publishes an unvalidatable zone file.

6.2.5.2. Risk Factors to Analyze

6.2.5.2.1. Threat Sources

- Key hardware, software, process failure

6.2.5.2.2. Vulnerabilities

- Malicious or unintentional (erroneous) alteration of root or TLD DNS configuration information
- Vulnerabilities arising from missing or ineffective security controls

6.2.5.2.3. Predisposing Conditions that Reduce Risk

- Emphasis on resiliency and redundancy
- Security project and program management skills/capacity
- Managerial vs operational vs technical security skills/focus/resources
- Diverse operational environments and approaches

6.2.5.2.4. Predisposing Conditions that Increase Risk

- Reliance on immature or custom built DNSSEC technologies
- Chain of trust single point of failure

6.2.5.2.5. Missing or Insufficient Security Controls

- Awareness and Training
- System and Information Integrity
- Incident Response

6.2.5.2.6. Threat Events

- Zone does not resolve or is not available

6.2.5.2.7. Adverse Impacts

In the worst case there would be broad harm/consequence/impact to operations, assets, individuals, other organizations and the world if any of these threat-events occur. And in all cases there would be significant problems for registrants and users in the zone.

6.3. Background materials and bibliography

[Action: clean up the mind-map and insert useful bits]

6.4. Methods – Rationale, selection, details

6.4.1. Rationale

Using a predefined methodology will save time and improve our work product

Consistent terminology
Shared model
Structured work
Sample deliverables

Reviewed several dozen alternatives -- We selected this one because it's:

Available at no cost
Actively supported and maintained
Widely known and endorsed in the community
Reusable elsewhere in ICANN

6.4.2. Selection

Methods evaluated

- A&K Analysis - ISO 17799
- Austrian IT Security Handbook
- BSI - IT-Grundschutz
- EBIOS - ISO 17799
- Hazard Analysis -- Critical Control Point (HACCP)
- HITRUST Common Security Framework
- ISAMM
- ISO/IEC 13335-2 (27005)
- ISO/IEC 17799
- ISO 27000 series
- ISO 31000 series
- Marion

- NIST 800-30
- OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)

6.4.3. Source documents

[cut/paste introduction and overview diagram from methods]

Link to source documents -- http://csrc.nist.gov/publications/PubsSPs.html

- NIST 800-30 DRAFT Guide for Conducting Risk Assessments
- NIST 800-53 Rev. 4 – DRAFT Security and Privacy Controls
- NIST 800-53A – Guide for Assessing Security Controls

6.4.4. DSSA-tailored framework

6.4.4.1. Risk-assessment worksheet

6.4.4.2. Components and scales

Table D7 -- Adversarial Threat Sources

- International governance/regulatory bodies
- Nation states
- Rogue elements
- Geo-political groups
- External parties and contractors
- Insiders
- Organized crime

Table D-3 -- Adversary capability

10 -- Very High -- The adversary has a very sophisticated level of expertise, is well-resourced, and can generate opportunities to support multiple successful, continuous, and coordinated attacks.
8 -- High -- The adversary has a sophisticated level of expertise, with significant resources and opportunities to support multiple successful coordinated attacks.
5 -- Moderate -- 5 -- The adversary has moderate resources, expertise, and opportunities to support multiple successful attacks.
2 -- Low -- The adversary has limited resources, expertise, and opportunities to support a successful attack.
1 -- Very Low -- The adversary has very limited resources, expertise, and opportunities to support a successful attack.

Table D-4 -- Adversary intent

10 -- Very High -- The adversary seeks to undermine, severely impede, or destroy the DNS by exploiting a presence in an organization's information systems or

infrastructure. The adversary is concerned about disclosure of tradecraft only to the extent that it would impede its ability to complete stated goals.
8 -- High -- The adversary seeks to undermine/impede critical aspects of the DNS, or place itself in a position to do so in the future, by maintaining a presence in an organization's information systems or infrastructure. The adversary is very concerned about minimizing attack detection/disclosure of tradecraft, particularly while preparing for future attacks.
5 -- Moderate -- The adversary actively seeks to obtain or modify specific critical or sensitive DNS information or usurp/disrupt DNS cyber resources by establishing a foothold in an organization's information systems or infrastructure. The adversary is concerned about minimizing attack detection/disclosure of tradecraft, particularly when carrying out attacks over long time periods. The adversary is willing to impede aspects of the DNS to achieve these ends.
2 -- Low -- The adversary seeks to obtain critical or sensitive DNS information or to usurp/disrupt DNS cyber resources, and does so without concern about attack detection/disclosure of tradecraft.
1 -- Very Low -- The adversary seeks to usurp, disrupt, or deface DNS cyber resources, and does so without concern about attack detection/disclosure of tradecraft.

Table D-5 -- Adversary targeting

10 -- Very High -- The adversary analyzes information obtained via reconnaissance and attacks to persistantly target the DNS, focusing on specific high-value or mission-critical information, resources, supply flows, or functions; specific employees or positions; supporting infrastructure providers/suppliers; or partnering organizations.
8 -- High -- The adversary analyzes information obtained via reconnaissance to target persistently target the DNS, focusing on specific high-value or mission-critical information, resources, supply flows, or functions, specific employees supporting those functions, or key positions.
5 -- Moderate -- The adversary analyzes publicly available information to persistantly target specific high-value organizations (and key positions, such as Chief Information Officer), programs, or information.
2 -- Low -- The adversary uses publicly available information to target a class of high-value organizations or information, and seeks targets of opportunity within that class.
1 -- Very Low -- The adversary may or may not target any specific organizations or classes of organizations.

Table D8 -- Non-Adversarial Threat Sources

INDIVIDUAL AND ORGANIZATIONAL SOURCES

- International governance/regulatory bodies
- Nation states
- Privileged users
- Key providers

ROOT-RELATED SOURCES

- Alternate DNS roots
- Root scaling (SAC 46)
- Intentional or accidental results of DNS blocking (SAC 50)

INFRASTRUCTURE-RELATED SOURCES

- Widespread infrastructure failure
- Key hardware failure
- Earthquakes
- Hurricanes
- Tsunami
- Blackout/Energy Failure
- Snowstorm/blizzard/ice-storm

Table D-6 -- range of effect (to DNS providers)

10 -- sweeping, involving almost all DNS providers
8 -- extensive, involving most DNS providers (80%?)
5 --wide-ranging, involving a significant portion of DNS providers (30%?)
3 --limited, involving some DNS providers
1 -- minimal, involving few if any DNS providers

Table E5 - Threat Events

- Zone does not resolve or is not available
- Zone is incorrect or does not have integrity

Table G2 -- Likelihood of Initiation -- by adversarial threat-sources

10 -- Very High -- Adversary is almost certain to initiate the threat-event
8 -- High -- Adversary is highly likely to initiate the threat event
5 -- Moderate -- Adversary is somewhat likely to initiate the threat event
2 -- Low -- Adversary is unlikely to initiate the threat event
0 -- Very Low -- 0 -- Adversary is highly unlikely to initiate the threat event

Table G3 -- Likelihood of Initiation -- by non-adversarial threat-sources

10 -- Very high -- Error, accident, or act of nature is almost certain to occur; or occurs more than 100 times a year.
8 -- High -- Error, accident, or act of nature is highly likely to occur; or occurs between 10-100 times a year.
5 -- Moderate -- Error, accident, or act of nature is somewhat likely to occur; or occurs between 1-10 times a year.
2 -- Low -- Error, accident, or act of nature is unlikely to occur; or occurs less than once a year, but more than once every 10 years.

0 -- Low -- Error, accident, or act of nature is highly unlikely to occur; or occurs less than once every 10 years.

Table F3 - Vulnerabilities

MANAGERIAL VULNERABILITIES

- Interventions from outside the process
- Poor inter-organizational communications
- External relationships/dependencies
- Inconsistent or incorrect decisions about relative priorities of core missions and business functions
- Lack of effective risk-management activities
- Vulnerabilities arising from missing or ineffective security controls
- Mission/business processes (e.g., poorly defined processes, or processes that are not risk-aware)
- Security architectures (e.g., poor architectural decisions resulting in lack of diversity or resiliency in organizational information systems)

OPERATIONAL VULNERABILITIES

- Infrastructure vulnerabilities
- Business continuity vulnerabilities
- Malicious or unintentional (erroneous) alteration of root or TLD DNS configuration information
- Inadequate training/awareness
- Inadequate incident-response

TECHNICAL VULNERABILITIES

- UNDER DISCUSSION
    - IDN attacks (lookalike characters etc. for standard exploitation techniques)

SYSTEM AND NETWORK VULNERABILITIES

- Recursive vs. authoritative nameserver attacks
- DDOS
- Email/spam

IDENTIFICATION AND AUTHENTICATION VULNERABILITIES

- Data poisoning (MITM, Cache)
- Name Chaining (RFC 3833)
- Betrayal by Trusted Server (RFC 3833)
- Authority or authentication compromise
- Packet Interception

- Man in the middle
- Eavesdropping combined with spoofed responses

TABLE F-2: ASSESSMENT SCALE - VULNERABILITY SEVERITY

10 -- Very High -- Relevant security control or other remediation is not implemented and not planned; or no security measure can be identified to remediate the vulnerability.
8 -- High -- Relevant security control or other remediation is planned but not implemented.
5 -- Moderate -- Relevant security control or other remediation is partially implemented and somewhat effective.
2 -- Low -- Relevant security control or other remediation is fully implemented and somewhat effective.
1 -- Very Low -- Relevant security control or other remediation is fully implemented, assessed, and effective.

Table F6 - Predisposing Conditions

MANAGERIAL

- Legal standing (and relative youth) of ICANN
- Multi-stakeholder, consensus-based decision-making model
- Managerial vs. operational vs. technical security skills/focus/resources
- Definitions of responsibility, accountability, authority between DNS providers
- Security project and program management skills/capacity
- Common ("inheritable") vs. hybrid vs. organization/system-specific controls
- Mechanisms for providing (and receiving) risk assurances, and establishing trust-relationships, with external entities
- Contractual relationships between entities

OPERATIONAL

- Diverse, distributed system architecture and deployment
- Emphasis on resiliency and redundancy
- Culture of collaboration built on personal trust relationships
- Diverse operational environments and approaches

TECHNICAL

- Requirement for public access to DNS information
- Requirements for scaling

Scales (enhanced by DSSA) to address whether the condition helps or hurts in the scenario

TABLE F-5a: ASSESSMENT SCALE - PERVASIVENESS OF PREDISPOSING CONDITIONS THAT POSITIVELY IMPACT RISK

.1 -- Very High -- Applies to all organizational missions/business functions
.3 -- High -- Applies to most organizational missions/business functions
.5 -- Moderate -- Applies to many organizational missions/business functions
.8 -- Low -- Applies to some organizational missions/business functions
1 -- Very Low -- Applies to few organizational missions/business functions

TABLE F-5b: ASSESSMENT SCALE - PERVASIVENESS OF PREDISPOSING CONDITIONS THAT NEGATIVELY IMPACT RISK

10 -- Very High -- Applies to all organizational missions/business functions
8 -- High -- Applies to most organizational missions/business functions
5 -- Moderate -- Applies to many organizational missions/business functions
3 -- Low -- Applies to some organizational missions/business functions
1 -- Very Low -- Applies to few organizational missions/business functions

Table F9 - Controls

MANAGEMENT CONTROLS

- Security Assessment and Authorization
- Planning
- Risk Assessment
- System and Services Acquisition
- Program Management

OPERATIONAL CONTROLS

- Awareness and Training
- Configuration Management
- Contingency Planning
- Incident Response
- Maintenance
- Media Protection
- Physical and Environmental Protection
- Personnel Security
- System and Information Integrity

TECHNICAL CONTROLS

- Access Control
- Audit and Accountability

- Identification and Authentication
- System and Communications Protection

TABLE F-9a: ASSESSMENT SCALE - PERVASIVENESS OF CONTROLS

10 -- Controls are missing
8 -- Controls are acknowledged as needed
5 -- Controls are planned or being implemented
2 -- Controls are implemented
1 -- Controls are effective

Table H3 -- Amount of impact

In the worst case there would be broad harm/consequence/impact to operations, assets, individuals, other organizations and the world if any of these threat-events occur. And in all cases there would be significant problems for registrants and users in the zone.

Since the potential impact values for confidentiality, integrity, and availability may not always be the same in different contexts/circumstances, the "high water" concept is used to determine the impact level. Thus, a low-impact system is defined as an information system in which all three of the security objectives are low. A moderate-impact system is an information system in which at least one of the security objectives is moderate and no security objective is greater than moderate. And finally, a high- impact system is an information system in which at least one security objective is high. It is our conclusion that the DNS is a high-impact system because the goals for integrity and availability are high.

Table H5 -- Adverse impacts

HARM TO NATIONS AND THE WORLD; E.G.

- Damage to a critical infrastructure sector
- Loss of government continuity of operations.
- Relational harms.
- Damage to trust relationships with other governments or with nongovernmental entities.
- Damage to national reputation (and hence future or potential trust relationships).
- Damage to current or future ability to achieve national objectives.

HARM TO INDIVIDUALS; E.G.

- Identity theft (only applies to "loss of integrity" threat-event)
- Loss of Personally Identifiable Information (only applies to "loss of integrity" threat-event)
- Injury or loss of life

- Damage to image or reputation.

HARM TO OPERATIONS/ORGANIZATIONS; E.G.

- Inability to perform current missions/business functions.
    - In a sufficiently timely manner.
    - With sufficient confidence and/or correctness.
    - Within planned resource constraints.
    - Inability, or limited ability, to perform missions/business functions in the future.
        - Inability to restore missions/business functions.
        - In a sufficiently timely manner.
        - With sufficient confidence and/or correctness.
        - Within planned resource constraints.
- Harms (e.g., financial costs, sanctions) due to noncompliance.
    - With applicable laws or regulations.
    - With contractual requirements or other requirements in other binding agreements.
- Direct financial costs.
- Damage to trust relationships or reputation
    - Damage to trust relationships.
    - Damage to image or reputation (and hence future or potential trust relationships).
- Relational harms.
- Harm to other organizations

HARM TO ASSETS; E.G.

- Damage to or of loss of information assets.
- Loss of intellectual property (only applies to "loss of integrity" threat-event)
- Damage to or loss of physical facilities.
- Damage to or loss of information systems or networks.
- Damage to or loss of information technology or equipment.
- Damage to or loss of component parts or supplies.

6.5. Guideline for handling Confidential information

6.5.1. Charter Guidelines

6.5.1.1. Principles

The DSSA-WG Charter recognizes that sub-groups may need to access sensitive or proprietary information in order for the DSSA-WG to do its work. These procedures are an exception to accountability and transparency standards. The DSSA-WG Charter does not require that members sign a formal Affirmation of Confidentiality and non-disclosure agreement (NDA) for membership in the DSSA-WG.

The primary goal of these guidelines is to make sure that the people sharing highly sensitive information with sub-groups are assured that their information will not find its way out of those sub-groups without their permission.

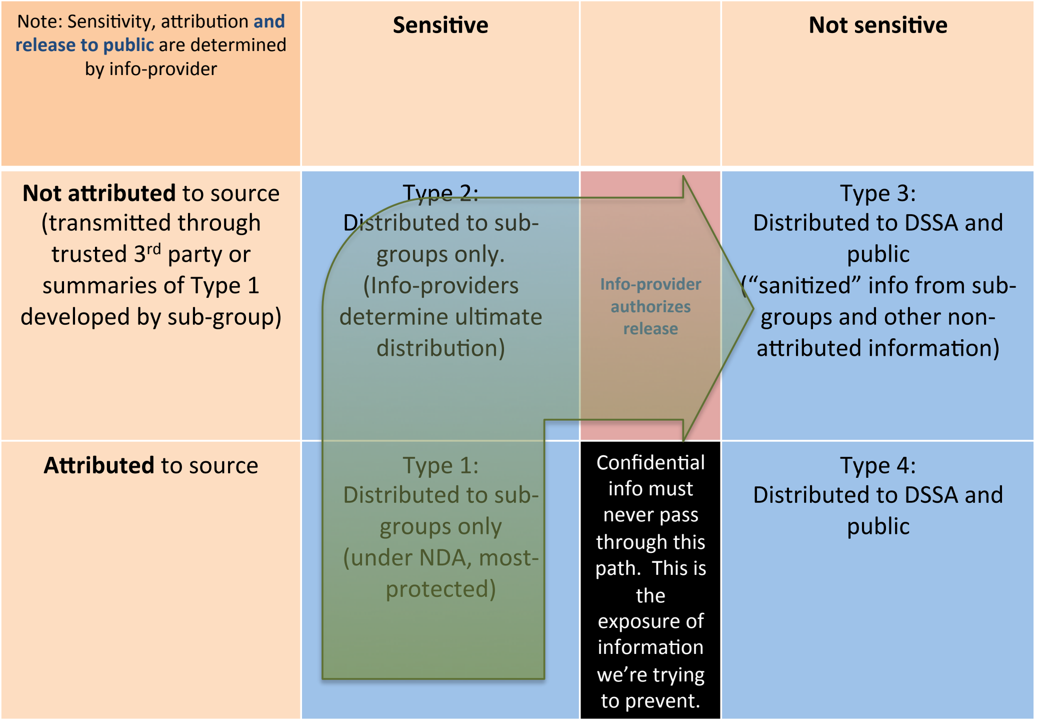
6.5.1.2. Sub-Groups

Sub-groups of the DSSA-WG may need to access sensitive or proprietary information in order for the DSSA-WG to do its work. Thus, measures may need to be established to access and protect confidential or proprietary information. The following procedures, as set forth in the DSSA-WG Charter, are an exception to the standards for transparency and accountability and only apply in cases where members of the aforementioned sub-groups of the DSSA-WG need to access and to protect confidential information:

- In certain cases under this exception, in order to ensure access to and protection of confidential or proprietary information, sub-groups' members of the DSSA-WG will be asked to sign a Formal Affirmation of Confidentiality and Non-Disclosure (See Annex B of the Charter). In addition, the sub-groups' members of the DSSA-WG may be required to sign a Non-Disclosure Agreement (NDA) for a specific project or issue.
- No formal Non-Disclosure Agreement (NDA) is required for membership in the DSSA-WG; and
- A separate email distribution list that is not publicly accessible may be established only to include the sub-groups' members who have signed a Non-Disclosure Agreement applicable to that specific project or issue.
- Information-providers may specify additional changes to these Guidelines after they've begun participating in a sub-group. The goal here is to ensure that information-providers do not find themselves trapped in an insecure situation with no mechanism to fix an unanticipated problem.

6.5.2. Dimensions of the information to be protected

This section addresses the sources and types of information that are addressed by these Guidelines.



Note: Sensitivity, attribution **and release to public** are determined by info-provider	**Sensitive**		**Not sensitive**
Not attributed to source (transmitted through trusted 3rd party or summaries of Type 1 developed by sub-group)	Type 2: Distributed to sub-groups only. (Info-providers determine ultimate distribution)	**Info-provider authorizes release**	Type 3: Distributed to DSSA and public (“sanitized” info from sub-groups and other non-attributed information)
Attributed to source	Type 1: Distributed to sub-groups only (under NDA, most-protected)	Confidential info must never pass through this path. This is the exposure of information we’re trying to prevent.	Type 4: Distributed to DSSA and public

6.5.2.1. Sensitivity

DSSA-WG members may be provided certain technical data or information that is commercially valuable and not generally known in its industry of principal use (collectively referred to as “Proprietary Information”) pursuant to the DSSA-WG’s performance of its tasks. As described in Annex B of the Charter, DSSA-WG members will use reasonable care to hold in confidence and not disclose any Proprietary Information disclosed to them. Written information provided to DSSA-WG members shall be considered Proprietary Information—i.e. information that is considered sensitive—if it is clearly marked with an appropriate stamp or legend as Proprietary Information. Non-written information shall be considered Proprietary Information only if the discloser of such information informs the DSSA-WG at the time of disclosure that the information being disclosed is of a proprietary nature.

DSSA-WG members have no obligation of confidentiality with respect to information disclosed to them if:

- Such information is, at the time of disclosure, in the public domain or such information thereafter becomes a part of the public domain without a breach of this Affirmation; or
- Such information is known to the DSSA-WG at the time it is disclosed; or

- Such information was independently developed by the DSSA-WG; or
- Such information is received by the DSSA-WG from a third party who had a lawful right to disclose such information to it; or
- The disclosing party provides written consent that the information is no longer confidential.

6.5.2.2. Nature

The nature of information falls into three general categories: data for analysis, information about internal processes, and information relating to trade secrets. In each case, whether this information is deemed to be Proprietary Information will be based on the decision made by the person providing the information. If the information is deemed to be Proprietary Information handling the information may require compartmentalization across sub-groups. As noted in Section 2.1 above, regardless of the nature of the information, Proprietary Information must be clearly marked with an appropriate stamp or legend as Proprietary Information. Non-written information shall be considered Proprietary Information only if the discloser of such information informs the DSSA-WG at the time of disclosure that the information being disclosed is of a proprietary nature.

6.5.2.3. Attribution

There are two options for attribution: either to attribute the information to its source or not to attribute it to its source. In each case, the provider of the information should make the decision and inform the DSSA-WG when providing the information. However, in some cases non-attributed information may be transmitted to the DSSA-WG through a trusted third party or from a sub-group to the DSSA-WG.

6.5.2.4. Distribution

There are two options for the distribution of information provided to the DSSA-WG. If the information is not proprietary, it may be distributed to the public. If the information is Proprietary Information, it may be distributed only to those DSSA-WG member and sub-group members who have signed a formal Affirmation of Confidentiality and NDA. For Proprietary Information distributed to sub-groups, the members of the sub-groups in coordination with the provider of the information shall decide whether the information may be distributed to the full DSSA-WG or elsewhere. The provider of the Proprietary Information shall make the final determination as to whom the information is distributed.

6.5.2.5. Use Cases

The following are the four types of use cases for information:

Type 1

- Sensitive, attributed

- Distribution to sub-groups only
- Governed/enforced by DSSA NDA (and project/use-specific NDAs if needed)
- Highest standard of protection

Type 2

- Sensitive, non-attributed
- Distribution to sub-groups only
- Transmitted through trusted third party or summaries of Type 1 information developed by sub-group
- Sub-group determines ultimate distribution, but the information providers have final say on "sanitized" versions of information they've submitted

Type 3

- Not sensitive, not attributed
- Distributed to the DSSA-WG and ultimately the public (via email list, wiki, report, etc.)
- "Sanitized" information developed by sub-groups
- Primarily Type 2 information that has been approved for release by the sub-group that developed it

Type 4

- Not sensitive, attributed
- Distributed to the public (via email list, wiki, report, etc.)

6.5.2.6. Data Repository

The sub-group may determine that it is useful to track the nature and status of confidential information that it receives. This is a preliminary description of what such a repository could entail. The DSSA is in continuing discussion on this item and may have additional suggestions and tools at the time that the sub-group is formed.

If the sub-group elects to establish a repository, it should be managed by a single trusted member of the sub-group.

Possible Content

- A copy of the confidential information itself (wording to be validated by the source)
- Source
- Date provided
- Mechanism by which source provided the information (e.g. email, verbally in a teleconference)
- Attribution (whether it can be attributed or not)
- Releasability (who this information can be released to)

- Distribution (who this information has been released to, when it was released, how it was released e.g. email, verbally in a teleconference, etc)
- List of any NDAs signed
- Change of status (e.g. some information may become less sensitive after a period of time, or information was withdrawn by the source)

6.5.2.7. Forming Sub-Groups

The following are the procedures for forming sub-groups in the DSSA-WG.[2]

The DSSA-WG may deem it suitable to ask for an existing group that is organized outside of ICANN to provide information back to the DSSA-WG. This group would be responsible for the accuracy, truthfulness, and allowable details of the threat but follow its own roles for handling of confidential information.

[2] When considering its guidelines for forming sub-groups the DSSA-WG consulted with the DNS Operations, Analysis, and Research Center (DNS-OARC) concerning its procedures. The DNS-OARC procedures follow these steps:

1. Describe/charter/document the group;
2. Documentation includes accepted rules of behavior;
3. "Seed" the group with highly-trusted core members;
4. Ask people to volunteer;
5. Publish/update the list of self-identified volunteers and request "vouches" from existing group members;
6. Group-members vouch for volunteers;
7. Admit volunteers that reach the threshold number of "vouches";
8. Monitor group membership and "vouches" to ensure that all members are above the minimum; and
9. Remove members who fall below the number-of-vouches threshold -- either because the people who vouched for them have left the group, or “vouches” are withdrawn after bad behavior.

The DSSA-WG has developed its procedures for forming sub-groups that incorporate some, but not all, of the aspects of those adopted by the DNS-OARC.

6.5.2.8. Sub-Group Charter and Membership-Selection

The Charter for each sub-group shall be the same as that of the DSSA-WG. The Sub-group members shall follow the rules of behavior set forth in the DSSA-WG Charter in addition to provisions for signing the Affirmation of Confidentiality and NDA, as applicable.

Initial sub-group members shall be selected by the Co-Chairs of the DSSA-WG in conjunction with information-providers (sometimes those discussions may be held in private) to include members solicited from the DSSA-WG, members who are acting as proxies and/or advocates for one or more information-provider, and outside experts who may have relevant information to provide relating to the issue(s) to be considered by the sub-group.

The DSSA-WG Secretariat shall publish the list of initial sub-group members. If additional sub-group members are needed beyond the initial list, new members can be proposed by any sub-group member. If further members are needed the DSSA-WG Secretariat also may send out a call for volunteers. For any additional new member to a sub-group the Secretariat shall ask the existing sub-group members to vouch for them. Volunteers will be admitted to the sub-group when two sub-group members have vouched for them and if they are acceptable to all of the information-provider members of the sub-group.

The size of the sub-group will be kept as small as possible in order to reduce the risk of information disclosure.

6.5.2.9. Sub-Group Roles

The following are the acceptable roles for the members of sub-groups:

1. Information-provider
2. Topic expert
3. Analyzer
4. Document-developer
5. Sub-group leader

6.5.2.10. Leaving the Sub-Group

Sub-group members will be removed if:

- They violate the Rules of Behavior in the Charter,
- Any information-provider sub-group member requests that they be removed from the sub-group, or

- They no longer have at least two sub-group members who have vouched for them (note: these vouching members can change, there just need to be two of them at any given time).

Any member may withdraw from a sub-group at any time. This is primarily aimed at information-providers who are no longer confident that they can participate in a way that maintains the confidentiality of their information, but applies to any member of the sub-group. Leaving the sub-group does not relieve the person of their responsibilities under any confidentiality agreements they've signed. If an information-provider leaves a sub-group, then perhaps they should specify whether the information already provided can continue to be used, or is withdrawn.

Membership in the DSSA-WG and the sub-groups will be monitored by the Secretariat.

6.6. Glossary

Adversarial threat source Individuals, groups, organizations or states that seek to exploit the DNS's dependence on cyber resources

Adverse Impact The harm to individuals and organizations that may occur as the result of a threat-event

Non-adversarial threat source Errors by individuals during the course of their everyday responsibilities, failures of equipment or software, and natural disasters and failures of critical infrastructure on which the DNS depends but which are outside the control of the providing/supporting organizations

Predisposing Conditions -- that positively or negatively impact risk A condition that exists within the DNS which contributes to (i.e., increases or decreases) the likelihood that one or more threat events, once initiated, result in undesirable consequences or adverse impact to organizational operations and assets, individuals, other organizations, or the world.

Risk -- to the DNS A measure of the extent to which the DNS is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. Note: these risks are those risks that arise from the loss of confidentiality, integrity, or availability of the DNS and reflect the potential adverse impacts to: operations (including mission, functions, image, or reputation), assets, individuals, other organizations, and the world.

Security Controls The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

Threat Event An event or situation that has the potential for causing undesirable consequences or impact.

Vulnerability Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.

6.7. Contact information

6.7.1. DSSA

6.7.2. Intermediaries for submitting information anonymously