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

Guidelines for Access to and Protection of Confidential Information

DRAFT 21, April 2012

1. Charter Guidelines

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.

1.2 Sub-Groups

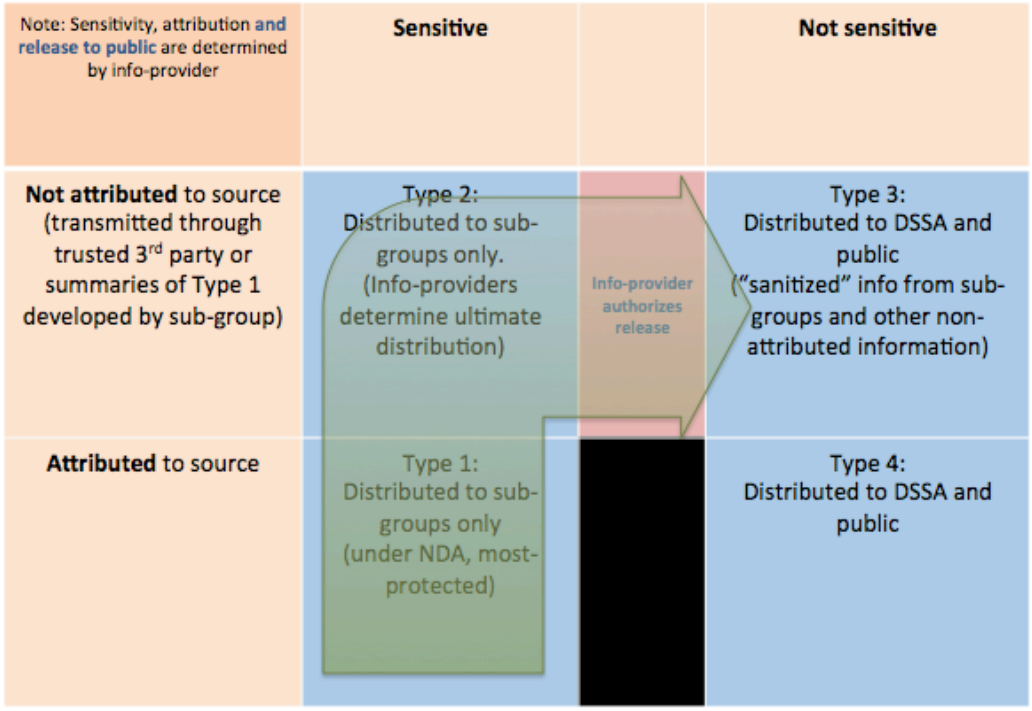
Sub-groups of the DSSA-WG may need to access sensitive or proprietary information in order for the DSSA-WG to do its work. Thus, measures may need to be established to access and protect confidential or proprietary information. The following procedures, as set forth in the DSSA-WG Charter, are an exception 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.

Information Overview



2. Dimensions

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.

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.

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.

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.

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.)

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)

3. Forming Sub-Groups

The following are the procedures for forming sub-groups in the DSSA-WG.[1]

[1] 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;

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.

3.1 Sub-Group Charter and Membership-Selection

The Charter for each sub-groups 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 could 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.

---

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.

3.1.1 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

3.1.2 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.