Forum of Incident Response and Security Teams (FIRST) Information Exchange Policy Special Interest Group Call for Participation

1. Background

Automating the exchange of security and threat information in a timely manner is crucial to the future and effectiveness of the security response community.

The timely distribution of sensitive information will only thrive in an environment where both producers and consumers have a clear understanding of how shared information can and cannot be used, with very few windows of interpretation.

The policy and governance aspects of automating information exchange are just as complex and nuanced as the technical challenges.

The general lack of adequate policy that supports information exchange is increasingly becoming an impediment to timely sharing. This will only be exacerbated as more organizations start actively participating in information exchange communities and the volume of security and threat information being shared continues to grow.

The Traffic Light Protocol (TLP) is the most commonly used method to mark and protect information that is shared. The original intent behind TLP was to speed up the time-to-action on shared information by pre-declaring the permitted redistribution of that information, reducing the need for everyone to ask the producer if it could be "shared with XYZ in my organization" and for that purpose TLP still works.

The challenge for producers of information is they need to be able to convey more than just the permitted redistribution of the information and there is a lack of clarity when defining and interpreting the permitted actions and uses of information shared between organizations. This is compounded by the sensitive nature and commercially competitive aspects of security and threat information.

Automating information exchange is not just a matter of technology; but also one of policy, language, and structured understanding.

2. FIRST IEP-SIG Goals and Deliverables

The need for a common IEP framework has been identified and the FIRST IEP-SIG has been formed to collaboratively develop an extensible IEP framework.

The goal of the IEP-SIG is to promote information exchange more broadly by defining an extensible IEP framework that removes the ambiguity related to information exchange expectations, obligations, requirements, and restrictions.

The intent of the IEP-SIG is not to constrain or dictate the policies that organizations must support or conform to, but rather to collectively address this problem and define a baseline of common policy elements and definitions that could help avoid the future need to support and translate a multitude of policy frameworks.

The main deliverable for the IEP-SIG is to create a framework document that includes common definitions that can be reused in sharing agreements and policies, and to define recommended practices.

3. IEP-SIG Participation

Anyone can participate in the IEP-SIG, including organizations who are not members of FIRST, and we would like a global representation and cross section of participants including National CERTs, incident responders, security vendors, community stewards, policy writers, and lawyers.

If you would like to join the IEP-SIG then please email the FIRST Secretariat **first-sec@first.org**.

FIRST Uniform Intellectual Property Rights Policy
Participation in the IEP-SIG requires that the FIRST Uniform Intellectual Property Rights Policy has been signed by someone from the participant's organization, who is authorized to enter into this agreement.

IEP-SIG Meetings
The IEP-SIG will meet via conference call every two weeks starting 14 April, 2016. There will be two calls held on each meeting day to cater for the different time zones of FIRST members. Meeting details will be announced on the IEP-SIG mailing list.

The intention of the IEP-SIG is to finalize the first version of the IEP at an in-person meeting during the 28th Annual FIRST Conference (June 12–17, 2016). A final draft of the IEP will be published for comment, ahead of the FIRST conference.

IEP-SIG Co-Chairs
The IEP-SIG has four Co-Chairs to ensure we can hold two, time zone specific, conference calls on each IEP-SIG meeting day. The IEP-SIG Co-Chairs and authors of the draft IEP Framework v1.0 are:

- Merike Kaeo, Farsight Security
- Paul McKitrick, Microsoft
- Steve Mancini, Cylance
- Terry MacDonald, Cosive

4. IEP Framework

The initial IEP framework has been prepared to act as a starting point for discussion, it should not be viewed as the final framework, as there are a number of open questions that need to be answered.

The draft framework is the culmination of a number of informal discussions and meetings with people from across the security community that took place at various events and conferences over the past two years.

Acknowledgements
The IEP-SIG Co-Chairs would like to acknowledge the following people who have contributed to the discussions, planning, and/or the development of the draft framework, but note that this does not equate to endorsement of the framework and may not represent their individual views:

- Aharon Chernin
- Bill Smith
- Chris Camacho
- Chris Hale
- Dave Dittrich
- David Watson
- Katherine Carpenter
- Keith Miller
- Kevin Sullivan
- Lee Rock
- Matthew Bucher
- Merike Kaeo
- Paul McKitrick
- Paul Vixie
- Richard Perlotto
- Richard Struse
- Scott Brown
- Steve Mancini
- Terry MacDonald
- William Peteroy