NPCC Scope Expansion Form Guide

Revision No. 0
Effective Date: July 30, 2014
# TABLE OF CONTENTS

1.0 Introduction and Background .................................................................................................................. 3

2.0 General Guidance ........................................................................................................................................ 4
   Self-Report Form and Scope Expansion Form Differences .................................................. 4
   Scope Expansion Form Use ................................................................................................................. 4
   Scope Expansion Form Required Information .............................................................................. 4
   Example of Potential Scope Expansion ......................................................................................... 5

3.0 Revision History ......................................................................................................................................... 6
1.0 Introduction and Background

Introduction
This Scope Expansion Form Guide is intended to provide guidance to assist Registered Entities with the submission of Scope Expansion Forms. The guidance provided in this Scope Expansion Form Guide will provide Registered Entities with a better understanding of the information necessary for NPCC to provide efficient and timely resolution of open enforcement actions (OEA).

Once an instance of potential noncompliance has been identified, the actions taken by the Registered Entity can be as important as the facts that led to the potential noncompliance. In some cases the Registered Entity discovers additional information that will change the scope of an existing OEA. An expeditious scope assessment is critical to determine and mitigate any potential or actual risk to the bulk power system (BPS).

Background
NPCC’s ability as a Compliance Enforcement Authority (CEA) to efficiently arrive at a final determination with respect to areas of noncompliance is in part dependent on the quality of the information and the understanding of the existing scope and related mitigation.

NPCC developed the Scope Expansion Form Guide to describe the type and quality of information that must be submitted in order to allow for an expeditious and accurate expansion of scope determination.

The purpose of this guide is to explain the differences between a new Self-Report and an expansion of scope and to outline the details required for the Scope Expansion form.
2.0 General Guidance

Self-Report Form and Scope Expansion Form Differences
The Self-Report form is used for newly identified areas of noncompliance. The Scope Expansion form is used for expanding the scope of an existing Possible Violation (e.g., Self-Reports, Self-Certifications, Audit Findings, etc.).

The Self-Report form generates a new NERC and NPCC tracking number while the Scope Expansion Form does not generate tracking numbers. A suffix is added to the Regional tracking number for identifying each scope expansion; the NERC tracking number remains the same.

While the Self-Report form contains the information related to the noncompliance issue, the Scope Expansion form contains the newly discovered instance(s) information and the details around its impact to an existing Possible Violation.

Self-Report and Scope Expansion forms are both submitted through the NPCC Portal.

Scope Expansion Form Use

A quality Self-Report consists of identifying the Reliability Standard and Requirement at issue and provides enough description to allow the CEA to understand the nature, cause and duration of the potential noncompliance.

In some cases additional instances of noncompliance are identified by a Registered Entity after submitting a Self-Report. If this is the case, a Scope Expansion form should be used to identify the additional instance(s) and the potential and actual risk associate with the newly discovered instance(s).

Scope Expansion Form Required Information

- Associated Violation
- Date Possible Violation (expansion) was discovered
- Beginning Date of Possible Violation (expansion)
- Detailed description and cause of the Possible Violation (expansion)
- Whether mitigating activities are in progress or completed
  - Description of mitigating activities
  - Details to prevent recurrence
  - Date mitigating activities expected to be completed or were completed
- Actual Impact to Bulk Power System
- Detailed description of Actual Risk to Bulk Power System
Example of Potential Scope Expansion
Registered Entity, as a Balancing Authority, identified an expansion of scope associated with NPCC2013-123456, a CIP-007-1 R1 noncompliance issue. On December 8, 2013, Registered Entity discovered that 35 additional Cyber Assets located inside of an ESP did not undergo security controls testing as required by CIP-007 R1.

Description of Possible Violation (expansion):
Registered Entity, as a Balancing Authority, identified an expansion of scope associated with NPCC2013-123456, a CIP-007-1 R1 noncompliance issue. Registered Entity identified 35 Cyber Assets that were not tested for security controls degradation after a security update was installed. This update was assessed and implemented according to procedure; however, the update was rolled out on production and development simultaneously. On December 9, 2013, the Registered Entity discovered that the update removed the need for an open port that was previously used by the application for FTP file transfers. On December 19, 2013, the Registered Entity updated all ports and service baselines to reflect this port removal.

The issue was discovered on December 8, 2013, by a system administrator who was reviewing change control tickets. Ten of the Cyber Assets were non-critical workstations, while the remaining 25 where Critical Application Servers. The original Self-Report identified 20 Critical Cyber Assets that were not tested. The failure to test for security control degradation for the additional 35 devices results in an expansion of scope and an expansion of risk. The Registered Entity considers the risk of the additional instances reported unchanged from the original Self-Report submission.
### 3.0 Revision History

<table>
<thead>
<tr>
<th>Revision</th>
<th>Date</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>7/30/2014</td>
<td>Creation</td>
</tr>
</tbody>
</table>