January 7-8, 2014 LNPA WORKING GROUP ACTION ITEMS ASSIGNED:

NOTE: FOR THE FOLLOWING ACTION ITEMS THIS NUMBERING SCHEME APPLIES:

- **FIRST TWO DIGITS DESIGNATE THE MONTH OF THE LNPA WG MEETING/CALL**
- **SECOND TWO DIGITS DESIGNATE THE DAY OF THE LNPA WG MEETING/CALL**
- **THIRD TWO DIGITS DESIGNATE THE YEAR OF THE LNPA WG MEETING/CALL**
- **LAST TWO DIGITS DESIGNATE THE ACTION ITEM NUMBER**

LNPA WG PARTICIPANTS ACTION ITEMS:

010714-01 – All service providers and vendors who plan to implement the XML interface are to notify Neustar if an IP address is not sufficient to designate the XML connection address, and if not, why not and what designation would be preferable (e.g., URL)?

010714-02 REVISED – Service Providers and Vendors should review the M&P for certificate-related activities in the NPAC XML interface. The M&P can be found on the NPAC secure web site at the following URL:

https://www.npac.com/npac-user/access-connectivity/npac-xml-certificate-trust-authority

Additionally, section 3.3 (NPAC Use of Certificates) in the XIS describe how this works from an application perspective.

Reviewers should consult with their information security teams to make sure these procedures are acceptable. In the current process, the User supplies basic information to the NPAC Certificate Authority (CA) via email. This basic information makes up the distinguished name of the certificate, and includes the SPID, region and system type. The NPAC CA creates a User within the system for this request, and the requestor receives the logon URL and the login credentials in separate emails. Upon login, JavaScript code is downloaded to the User's web browser. This JavaScript code calls APIs within the User's browser to generate a public/private key pair. The public portion of this key pair is then sent to the NPAC CA. The NPAC CA combines this public key with the information associated with the User to generate a signed certificate that includes the public key and the distinguished name information (the spid, the region, and the system type). This signed certificate is then downloaded to the User's machine, where it is combined with the private key. The private key is generated on the User's machine and is never transmitted to the NPAC CA.

010714-03 – Neustar to provide an updated list of NPAC features that they consider possibilities for sun-setting by January 24, 2014. The list should include updates from the January 2014 LNPA WG discussion and a short descriptive paragraph for each. They will also identify the CMIP features that are not carried forward to XML. Neustar will send this out via the LNPA WG distribution list.

010714-04 – WG members are to be prepared to continue discussion of the potential sun-set list at the March 2014 LNPA WG meeting. WG will discuss benefit and need for each item on the list including level of effort for keeping or removing.

010714-05 – John Nakamura to identify the change order associated with recovery operations while not in recovery.

ACTION ITEMS REMAINING OPEN FROM PREVIOUS LNPA WG MEETINGS:

No Action Items remain open from previous meetings.