**Response to Sandia Review of WGQ/RMQ Standards**

11/11/2019

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Sandia Issue1** | **Sandia Report2** | **Issue Summary** | **NAESB Response** | **WGQ Standards created/modified in response to this issue** | **RMQ Standards created/modified in response to this issue** |
| 1 | BusOps | Ensure timely adoption of new technology versions and software patches | NAESB agrees with Sandia’s findings and has modified our standards to specify specific timelines where applicable, and in all other cases make change as soon as possible in coordination with trading partners.  | D2, D3, D5, D6, D32, D33, D34 | D3, D4, D7, D8 |
| 2 | BusOps | Timely notification of trading partners for version updates and delays | NAESB agrees with Sandia’s findings and has modified our standards to specify specific notification timelines where applicable, and in all other cases make change as soon as possible in coordination with trading partners.  | D2, D3, D5, D6 | D3, D4, D6, D7, D8 |
| 3 | BusOps | Update references to obsolete SSL encryption standard | NAESB agrees with Sandia’s findings and has modified our standards to specify TLS V1.2, and centralized such references to make future revisions easier. | D9, D12, D14, D19, D28, D29, D30, D32, D34, D35, D36, D39, D40, D44 | D20, D21, D23, D26, D36, D39. D40, D44 |
| 4 | BusOps | Major security bulletins should be considered for 30-day implementation  | NAESB agrees with Sandia’s findings and has modified our standards to specify specific notification timelines where applicable, and in all other cases make change as soon as possible in coordination with trading partners.  | D1, D2, D3, D5, D6 | D3, D4, D6, D7 |
| 5 | BusOps | The RMQ standards should include adoption of generally available version with 9 months | NAESB agrees with Sandia’s findings and has modified our standards to include specific versions that should be observed. Not, however, that the “9 month GA” timeline is relevant to WGQ web sites standards; the RMQ has no corresponding web site standards. | NA | D6, D7, D8 |
| 7 | BusOps | Standards should include guidelines for system security tools and system fail-over. | NAESB agrees with Sandia’s findings and has modified our standards to include both specific and broad adoption of system security measures, and specific notification and coordination during outages with effected trading partners.  | D3, D5 | D3, D4 |
| 9 | BusOps | The Standards should be reviewed and legacy software/version references removed. | NAESB agrees with Sandia’s findings and has modified our standards to both remove dated versions (specifically PGP) and centralized such references to make future revisions easier. | D15, D17, D37, D38, D46, D49, D51, D55, D57, D58, D60, D61 | D15, D17, D37, D38, D46, D49, D51, D55, D57, D58, D60, D61 |
| 10 | BusOps | Update references to obsolete SSL encryption standard (similar to Issue 3) | NAESB agrees with Sandia’s findings and has modified our standards to specify TLS V1.2, and centralized such references to make future revisions easier. | D9, D12, D14, D19, D28, D29, D30, D32, D34, D35, D36, D39, D40, D44 | D20, D21, D23, D26, D36, D39. D40, D44 |
| 11 | BusOps | Replace references to insecure HTTP communications with HTTPS. | NAESB agrees with Sandia’s findings and has modified our standards to specify HTTPS whenever secure communication is required. | D1, D9, D13, D16, D18, D27, D28, D29, D30, D40, D45 | D24, D25, D40, D45 |
| 12 | BusOps | Update/enhance encryption references to include a minimum 128-bit key length and SHA-2 or SHA-3 hash algorithms. | NAESB agrees with Sandia’s findings and has modified our standards to specify 128-bit key length, newer PGP versions and hash algorithms. | D12, D27, D53 | D53 |
| 13 | BusOps | Consider options to mitigate replay and amplification attacks | TBD |  |  |
| 4 | Add | Consider employing 2-factor authentication on an individual user level for secure web sites.  | NAESB agrees with Sandia’s findings that secure web sites should employ individual user credentials and have modified standards to comport with the finding. However, we find that the current standard of user IDs and passwords maintains the security of web sites without complicating the login process, especially for users that access multiple web sites. | D1, D9, D18, D29, D30, D40, D45 | D40, D45 |
| 5 | Add | Whitelisting | TBD |  |  |
| 10 | Add | Standards should encourage security assessments and coordination between customers and vendors. | NAESB agrees with Sandia’s findings and has modified our standards to encourage security assessments and coordination between customers, vendors and trading partners. | D1, D32, D33, D34 | D32, D33, D34 |
|  |  | Refnum | TBD |  |  |

1 Not all identified issues were relevant to WGQ/RMQ, so the issue numbering contains gaps.

2 BusOps = Business Operations Practices and Standards Report; Add = Addendum Report