Comments on BASE ICR (1652-0062) Revision

TSA Sends Detailed Info on Base ICR Changes to OMB – 9-8-21

Yesterday the OMB's Office of Information and Regulatory Affairs (OIRA) announced that it had received a 30-day information collection revision request from the Transportation Security Administration for their "Highway Baseline Assessment for Security Enhancement (BASE) Program" ICR. TSA published their 60-day ICR notice in June, and I filed comments upon that notice. The 30-day ICR notice was published two-weeks ago.

More Details on Cybersecurity Questions

As expected, TSA has provided significantly more information to OIRA about the new cybersecurity questions that it will be covering in its revised base. They provided OIRA with copies of the spreadsheets that will be used to collect the responses to the new questions. The four new spread sheets are:

Highway Cybersecurity New Question Set
Highway New Cybersecurity Annex
MTPR Cybersecurity New Question Set
MTPR New Cybersecurity Annex

NOTE: The links above are all download links of .xlsx files. MTPR – Mass Transit/Passenger Rail

In the Supporting Document (.docx download link) TSA explains that:

"As part of the new data collection requirements triggered by the GAO recommendations, TSA is revising the information collection to add 21 questions to both BASE assessments. The questions relate to an entities' cybersecurity program. The previous versions did not include the Detect and Recover functions of the NIST framework."

Thus, the 'New Question Set' spreadsheets documents the new 21 questions that all organizations will be asked to voluntarily answer as part of a TSA Surface Security Inspectors (TSAs-SI) BASE review. While the questions do not go into any great detail (to be fair, nor to any of the existing questions), the questions do address specific requirements of the NIST Cybersecurity Framework. For example, the figure below shows the question set for policies and procedures. All questions are of the 'yes' or 'no' response variety.

13.203	Has your organization established and documented policies and procedures for the following?	Data Security
	*Access Control	Data Security
	*Awareness and Training	Data Security
	*Audit and Accountability	Data Security
	*Configuration Management/Baseline security controls	Data Security
	*Cyber Asset Management and Maintenance/Change Management	Data Security
	*Cybersecurity Incident Response	Data Security
	*Identification and Authentication	Data Security
	*Information Protection	Data Security
	*Insider Threat	Data Security
	*Media Protection	Data Security
	*Patch Management	Data Security
	*Personnel Security	Data Security
	*Physical Protection (related to cyber systems, cyber assets, communications)	Data Security
	*Recovery (disaster, business continuity) plan(s)	Data Security
	*Risk Assessment	Data Security
	*Security Assessment	Data Security

Interestingly, these new questions do not link to the evaluation process used in the BASE Workbook {see the Highway Base Workbook (.xlsx download link)} for example. Those workbooks allow a TSA inspector to score the implementation responses to questions. The workbook takes those individual question scores and prepares a Comprehensive Summary of the overall security process implementation of the organization.

Cybersecurity Annex

In addition to the addition of the expanded cybersecurity questions loosely associated with the BASE assessment, TSA has also developed Cybersecurity Annexes for both Highway and MTPR organizations. According to the Supporting Document submitted to OIRA:

"Consistent with GAO's recommendation, TSA also developed a cybersecurity annex for the entities interested in a comprehensive, thorough assessment of their cybersecurity hygiene. The annex is voluntary and designed to complement the BASE program, but will be conducted independent of the BASE checklist. In adding the cybersecurity annex, TSA is revising the information collection by increasing the total number of questions to 87, where there are 21 BASE questions and 66 cybersecurity annex questions. This effort aligns with TSA's Cybersecurity Roadmap to gain a understanding of the national transportation cybersecurity posture, providing necessary information to assess and prioritize cybersecurity risks to the sector."

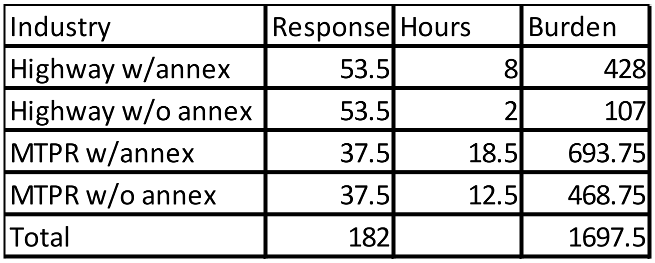
The question count is a little misleading, each of the questions in the BASE Checklist addendum are repeated in the Annex spread sheet. While the questions still require a 'yes' or 'no' response, they do cover a wide range, but not all, of the topics listed in the NIST Cybersecurity Framework. The linkage of the cybersecurity questions to the CSF, however, are questionable.

For example, the first four questions in the Highway Annex are listed under the heading "Identify" and the "NIST Category" column in the spread sheet shows "Asset Management". None of the four questions have anything to do with the six Identify/Asset Management listings in the CSF. The questions are legitimate items of cybersecurity concern, and many are similar to those addressed in the CSF, but the specific linkages alleged in the Annex do not exist.

While this is not a matter of concern for OIRA, the GAO will want to look at this closely when they evaluate whether these questions satisfy their recommendation to include CSF related questions in the BASE analysis.

Burden Assessment

The Support Document provides the following burden estimate:



Industry	Response	Hours	Burden
Highway w/annex	53.5	8	428
Highway w/o annex	53.5	2	107
MTPR w/annex	37.5	18.5	693.75
MTPR w/o annex	37.5	12.5	468.75
Total	182		1697.5

TSA estimates that they will conduct BASE assessments on 107 highway transportation organizations and 75 mass transit/passenger railroads each year. They expect that half of those contacted will be willing to complete the Cybersecurity Annex. This compares with the 90 and 75 annual assessments forecast in the current version of this ICR. TSA does not explain the reason for this increase.

Commentary

In my comment submitted in response to the 60-day ICR notice I complained that the TSA did not provide adequate information about the changes to the collection to allow industry to comment on the proposed burden assessment. Their response was included in the Support Document submitted yesterday to OIRA. They explained that the information was now available. So, that information is now available, and the public has until September 27th, 2021 to submit their comments to OIRA; this is substantially less that the 30-days required by 44 USC 3507(b).

It is very disappointing to see that while the TSA is including additional details on cybersecurity in its BASE information collection it is not taking any effort to include the responses to those questions in its assessment. It seems to me that lacking that assessment, the TSA does not have any reason to collect the new information. OMB should disapprove this revision to the information collection as the new burden is not necessary. The easiest way submit a comment that is to go to the ICR page and click on the 'Comment' button on that page.

I urge all highway transportation, mass transit, and passenger rail organizations to review the new data to provide feedback to OIRA about the adequacy of the burden assessment and the necessity of the data collection.

A copy of this article will be filed as a comment on this ICR.