CISA Publishes 60-Day ICR Revision Notice for Vulnerability Discovery Program

On Friday, DHS published a 60-day information collection request (ICR) revision notice in the Federal Register (86 FR 19499-14945) for the DHS Vulnerability Discovery Program (RIN #: 1601-0028).

The Information Collection

According to the notice:

"DHS is requesting pursuant to 44 US Code 3509 [link added], that the information collection be designated for any Federal agencies ability to utilize the standardized DHS online form to collect their own agency's vulnerability information and post the information on their own agency websites."

Each agency collecting information under this ICR would use the DHS collection form but would post it on the agency web site. The information collected will include:

• Vulnerable host(s),
• Necessary information for reproducing the security vulnerability,
• Remediation or suggestions for remediation of the vulnerability, and
• Potential impact on host, if not remediated.

DHS estimates no change in the burden due to this expansion of the coverage of the ICR.

Public Comments

DHS is soliciting public comment on this revision. Comments may be submitted via the Federal eRulemaking Portal (www.Regulations.gov; Docket # DHS-2021-0009). Comments should be submitted by May 18th, 2020.

Commentary

Earlier this month the OMB's Office of Information and Regulatory Affairs (OIRA) approved an emergency revision of this DHS ICR that would allow other Federal agencies to use the same ICR for their individual vulnerability discovery programs. That emergency approval came with the proviso that DHS submit an ICR revision in the normal manner to confirm the expanded collection effort. This is the direct response to that proviso.

In this notice DHS continues to rely on the 'information sharing' provisions of 44 USC 3553(l) (added by §1705(2) 1705 of PL 116-283). This language allows DHS to "access, use, retain, and disclose, and the head of an agency may disclose to the Secretary, information, for the purpose of protecting information and information systems from cybersecurity risks." That does not really pertain to collecting voluntarily supplied information from outside of the government for a vulnerability discover program. A more appropriate justification would be the newly added §3553(b)(8)(B) {added by §1705(1)}: that gives DHS authority for ") deploying, operating, and maintaining secure technology platforms and tools, including networks and common business applications, for use by the agency to perform agency functions, including collecting, maintaining, storing, processing, disseminating, and analyzing information [emphasis added]".

Unfortunately, this justification and the reliance in the Notice upon 44 US Code 3509, would seem to run counter to the concept of each agency collecting, processing and analyzing data from its own vulnerability discovery program using the DHS provided form. Section 3509 does allow OMB to "designate a central collection agency to obtain information for two or more agencies", but it specifically prohibits an agency from collecting "for itself information for the agency which is the duty of the collection agency to obtain." Thus, under §3509, DHS would run the data collection under the multi-agency VDP and either provide the raw data to the agency for processing and analysis or would provide the processed and/or analyzed data to the client agency for action. Neither of those options were described in this 60-day ICR notice.

One final objection to the data presented in this ICR revision request, it presents inadequate information on the burden of the data collection and this is arguably one of the most important parts of the ICR process. The current burden estimate is identical with the burden estimate for the DHS only Vulnerability Discovery Program that was approved by OIRA back in August of last year; 3,000 annual responses with an estimated time spent on each response being three hours for a total burden of 9,000 hours with a total annual responder cost of $647,280. It only seems reasonable to assume that a multi-agency VDP would have a larger number of responses, burden and cost.

Granted, DHS has not been running their own VDP long enough to have a solid history to even semi-accurately estimate the number of future responses that they would expect to receive in the future, but the ICR process demands that a reasonable effort be made to project the burden and revise the estimate in future renewals based upon actual program data.

At this point, DHS is not even sure how many agencies will be utilizing this DHS ICR to support their own program. So, what DHS should have probably done is to establish a reasonable estimate for an agency VDP for agencies of different sizes {eg, small (think FDA), medium (think DHS) and large (think HHS)} and then estimate the number of each size agency that will adopt the DHS VDP, calculating the burden from there. Subsequent ICR revisions would refine the future estimates from the collected data.