Food Protection and Defense Institute
A Homeland Security Center of Excellence

Homeland Security
Science and Technology

ADM

Intentional Adulteration Analysis Tool (IAAT) FAQs

- *How do I gain access to the IAAT program?*

  The IAAT, is a desktop tool that requires internet for both initial download and future updates. The Tool will be downloaded from the FoodSHIELD website (www.foodshield.org), which is owned and operated by FPDI through the University of Minnesota. FoodSHIELD will host the IAAT application, and tools for collaborative exchange and background information. Members of FoodSHIELD and newly identified users will be able to request access to the IAAT tool from the App Store, or via direct short link to supporting workgroup access request.

- *What is the IAAT?*

  The Intentional Adulteration Analysis Tool (IAAT) is a desktop application developed to aid food production facilities in an assessment of their processes' vulnerability and risk to intentional adulteration by a potential internal or external aggressor. Agents evaluated include acute toxic chemicals, biological toxins and pathogenic microbes. The Food Protection and Defense Institute (FPDI) has coded the CSAC-ADM vulnerability model into a prototype desktop software tool. The model takes into account the requirements for a vulnerability assessment within the FDA Intentional Adulteration rule.

  The Department of Homeland Security's Chemical Security and Analysis Center (CSAC), the Archer Daniels Midland Company (ADM) and FPDI are developing the tool collaboratively. CSAC and ADM entered into a Cooperative Research and Development Agreement (CRADA) to exchange information about each other's models and to co-develop an unclassified model broadly useful to the food industry at large.

- *Why was the program built as a desktop tool instead of a web-based application?*

  In order to allow industry to protect, store and update the assessments internally, a stand-alone, downloadable desktop application was developed instead of a web-based application. The downloadable software is designed to be installed on a company computer at the corporate facility. A knowledgeable individual enters the operational specifics of the food process into the software, which is then used to conduct vulnerability assessments on the food processing operation. The results of the vulnerability assessment can then be used with selected mitigation strategies to implement an appropriate food defense program.

- *What are the steps in building out the process?*

  Companies would start to build their process from their current HAACP flow diagram or flow chart from their Food Safety Plan. The IAAT user then defines each product with a name, serving size, and process line. A wizard guides the user through adding process steps.

For each step, the user inputs process parameters such as temperature, batch size, and rate and answers questions regarding the degree of access to a step.

- *How is the vulnerability estimate calculated?*

Vulnerability Estimates: The vulnerability is calculated for each agent at each step in the process model. The basis of the calculation is to multiply the following probabilities:

  - Probability the agent can be acquired (pAq) *
  - Probability that the step can be accessed by the aggressor (pAc), both internal and external aggressors are assessed*
  - Probability that the agent will survive the process (1-pELim) for the current and all subsequent process steps

$VE_{,1}$: The vulnerability estimate is calculated using inherent properties of the processing step (e.g. pAc=1 if the processing step can be accessed, pAc=0.00001 if the system is closed). Steps that result in a VE,1 value >0.001 are identified as Actionable Process Steps (APS).

$VE_{,2}$: The vulnerability estimate is calculated using pAc values based on existing facility measures such as access controls or mitigation strategies used at that step.

- *Is the IAAT aligned with the FDA Food Defense Plan Builder?*

FDA guidance on the IA rule and training materials are not available at this time. However, FDA has reported that they will be updating the Food Defense Plan Builder (FDPB) software. In the current version of the FDPB, the user assigns an accessibility and vulnerability score from 1-10 for each process step. The two scores are added together to create a vulnerability assessment score. Process steps can then be ranked in order of risk by their score. The user defines if the step is an actionable process step that requires a mitigation strategy. The IA rule requires that the facility look at vulnerability for both an internal and an external aggressor, which is not addressed in this version of the FDPB.

IAAT uses a more quantitative approach to assessing vulnerability by assigning probabilities to agent acquisition, accessibility, and then utilizes the agent database to calculate estimates on agent survival through the process steps. The three probabilities are used to calculate a vulnerability estimate for both an internal and external aggressor.

- *Recommendations on choosing a serving size?*

Serving size is used in the IAAT to calculate the potential number of servings impacted by an intentional adulteration event and the potential impact on public health based on toxicity data for each agent. Serving size should be based on the amount of product that would be consumed by a person according to label value, reference amount customarily consumed (RACC), or typical consumption data defined by the user. Serving size in the IAAT model is entered in grams.