# Integrated Adaptive Cyber Defense (IACD) Trust in Automation

## Why is trust in automation important for IACD?

**Whenever an organization invests in cyber defense automation, they must think about how trust in that automation impacts the organization's ability to defend itself from cyber attacks.**

Trust is a necessary component in realizing the full potential of cyber defense automation which is an integral part of IACD. Trust in automation is built through the implementation of well-designed automation, a properly trained and informed work force, and a pro-automation workplace culture with manageable workload. These factors encourage properly calibrated trust which contributes to appropriate reliance on automation and leads to valuable automation contributions in mitigating cyber incidents consistently at increased speed and scale while reducing risk.

## What are some ways to achieve trust in automation?

### Ensure automation supports trust

Certain automation traits can improve the comprehension and ease of use to increase the workforces' trust in and reliance on that automation. For example, automation which is accurate, reliable and repeatable, provides transparency into its actions, is understandable and sustainable, and projects a higher level of trustworthiness.

### Train and educate workforce

A well-trained workforce which is also educated on the philosophy of their work has the ability to understand the automation and work environment. This empowers the staff to calibrate their trust in the automation to best fit the situation.

### Trust-focused workplace culture

Workplace cultures that encourage the use of automation to increase productivity by leveraging automation's ability to do routine tasks quickly, thus allowing current personnel to focus on higher-level tasks, foster an environment that supports trust in and reliance on automation.

## How can organizations promote calibrated trust?

Calibration is the key to realizing the most potential from automation. Allowing excessive automation contribution *(becoming complacent and not properly monitoring automated activities)* results in costly errors that may be hard to detect and correct in a timely manner. Allowing no or limited automation contribution results in additional labor for the cyber defense personnel and reduces operations consistency. Organizations must ensure their automation supports trust with enabling trustworthiness, which leads to valuable automation contribution. This is accomplished by emphasizing personnel training on automation use as well as education regarding the mission, and also by cultivating a positive workplace culture that promotes proper calibration of trust and reliance.