2020 DON IM/IT Excellence Awards Nomination Criteria

Award Category	DON IM/IT Excellence Awards	DON IT Person of the Year & Rising Star of the Year Awards	Information System Security Manager (ISSM)/Information System Security Officer (ISSO) of the Year Award	Privacy Program Excellence Award	Freedom of Information Act (FOIA) Program Excellence Award
Number of Awards	2 – 4 Teams	1 Person of the Year; 1 Rising Star of the Year	1 Individual	1 Individual or Team	1 Individual or Team
Eligibility	Team that meets one or more of the criteria below (can include but not be led by contractors):	Individual who meets one or more of the criteria below (government civilian or military):	Individual government civilian or military that meets one or more of the criteria below:	Individual (gov't civilian or military) or team (can include but not be led by contractors) that meets one or more of the criteria below:	Individual (gov't civilian or military) or team (can include but not be led by contractors) that meets one or more of the criteria below:
Criteria	• **People:** Made significant contributions to the training of the military and civilian IT and Cybersecurity workforce • **Capabilities:** Demonstrated exceptional performance in modernization of key IT capabilities or working towards new technologies or Applied innovative concepts and/or challenged conventional thinking resulting in improved use of DON information or acceleration of an innovative concept. • **Processes:** Employed continuous improvement mindset, culture, or systems, delivering performance with affordability and speed or Contributed value to the organization by improving mission essential business processes.	• **Person of the Year**: GS13/O4/W-1/E-7 and above • **Rising Star of the Year**: GS-12/O3/E-6 and below • Same criteria as DON IM/IT Excellence Awards	• Actions resulted in significant improvements in cybersecurity program management, or enabled higher levels of cybersecurity, computer network defense, or identity management. • Responsible for ensuring timely implementation and completion of Risk Management Framework (RMF) authorization efforts. • Significant contributions to updating local cybersecurity policy and ensuring dissemination, exercises, and understanding by user community. • Identified a potential cybersecurity threat and through proactive actions, potentially stopped the infiltration of a DON network. • Efforts resulted in the highest marks ever granted (by an inspecting organization) to their organization as a result of a first pass Cybersecurity Inspection.	• Exhibited Superior leadership skills or high performing team, demonstrating a commitment to privacy, advancing the effectiveness of the command privacy program. • Contributed value to the command and employees by implementing processes that safeguard PII. • Promoted privacy training and awareness to all levels of the command. • Significantly reduced the collection and use of the SSN and other sensitive PII in business processes. • Improved program effectiveness through management controls including compliance spot checks, PIA compliance, SORN reviews and records disposal. • Implemented technology safeguards to reduce loss, theft or compromise of PII, including data loss prevention, data at rest, and network monitoring.	• Exhibited superior leadership or high performance demonstrating a commitment to freedom of information. • Contributed value to the organization by increasing efficiency, improving processes, providing training, or implementing technology that advances the freedom of information (e.g., prompt responsiveness, backlog reduction, proactive posting). • Increased awareness of DON services in furtherance of the Freedom of Information Act through effective public outreach. • Improved program compliance with DON policies in furtherance of the Freedom of Information Act through management controls and spot checks.