**AUSTIN SCOTT**
EIGHTH DISTRICT, GEORGIA

WARNER ROBINS OFFICE
120 BYRD WAY, SUITE 100
WARNER ROBINS, GA 31088
478.971.1776 MAIN
478.971.1778 FAX

TIFTON OFFICE
127 B NORTH CENTRAL AVENUE
TIFTON, GA 31794
229.396.5175 MAIN
229.396.5179 FAX

Congress of the United States
House of Representatives
Washington, DC 20515

HOUSE ARMED SERVICES COMMITTEE
SUBCOMMITTEE ON READINESS
SUBCOMMITTEE ON INTELLIGENCE, EMERGING THREATS AND CAPABILITIES

HOUSE COMMITTEE ON AGRICULTURE
CHAIRMAN
SUBCOMMITTEE ON COMMODITY EXCHANGES, ENERGY, AND CREDIT
SUBCOMMITTEE ON GENERAL FARM COMMODITIES AND RISK MANAGEMENT

HOUSE PERMANENT SELECT COMMITTEE ON INTELLIGENCE

October 5, 2023

Mr. John Sherman
Chief Information Officer
Department of Defense
6000 Defense Pentagon
Washington, D.C. 20301-6000

Dear Mr. Sherman:

It has come to my attention that the Department of Defense (DOD is procuring encrypted data storage products that utilize encryption technology developed and produced in the People's Republic of China (PRC). The provider of these chips is on the State Department's Entities List. Specifically, a subsidiary of Hualan Microelectronics, Sage Microelectronics, and another subsidiary, Initio (See Supplement 4 to Part 744 of the Export Administration Regulations) is producing and providing these encryption chips for inclusion in encrypted hard drive technology. Moreover, it is my understanding that at least three vendors to DOD (Apricorn, Istorage Limited, and SecureData) sell encrypted hard drives utilizing this technology.

As a member of the House Armed Services Committee (HASC) and the House Permanent Select Committee on Intelligence (HPSCI), I am very concerned about the potential for backdoors and the possibility of remote data access by the PRC. Additionally, I am concerned that classified data could be stored on data storage products using these PRC sourced chips. These are risks that I consider unacceptable, and feel must be addressed.

To that end, I request a written assessment of the extent of the penetration of this technology. Additionally, I would also seek in your written response on how DOD will fix this issue to ensure a clean supply chain for encryption chips. My point of contact is Jim Dolbow who can be reached at jim.dolbow@mail.house.gov. I look forward to working with you on this issue as we move forward and appreciate your immediate attention to this important matter.

Sincerely,

Austin Scott

Austin Scott
Member of Congress

**DEPARTMENT OF DEFENSE**
6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

CHIEF INFORMATION OFFICER

DEC 6 2023

The Honorable Austin Scott
Committee on Armed Services
U.S. House of Representatives
Washington, DC 20515

Dear Congressman Scott:

In your letter of October 5, 2023, you expressed concern over potential backdoor access risks in the DoD's acquisition of computer products containing microelectronics from Hualan Microelectronics, or any of its subsidiaries, and asked that DoD provide you with our assessment of:

1. "the extent of the penetration of this technology;" and
2. "how DoD will fix this issue to ensure a clean supply chain for encryption chips."

Hualan Microelectronics products (including products from its Sage Microelectronic and Initio subsidiaries) are embedded within various computer products such as hard drives, USB drives, and solid-state storage controllers produced by various original equipment manufacturers (OEMs) and provided by a variety of suppliers. These products are generally not sold separately or identified to the end-product purchaser. At this time, computer equipment OEMs are not required to provide a hardware Bill of Material itemizing the components and their provenance for the internal parts within their computer products. Thus, without supplier disclosure or some disassembly, identification of Hualan, Sage, or Initio internal parts included in computer products is not supported; the extent of Hualan-associated products use nested within various end-products, within a myriad of OEMs and suppliers, acquired by DoD is unknown.

Absent any new overarching legislative prohibitions on procuring, obtaining, or contracting for microelectronics from specified suppliers, DoD will continue to assess overall supplier and technology risks and apply a variety of risk management tools. These tools involve usage advisories and caveats, systems security engineering mitigations, and potentially acquisition exclusion in cases where mitigations are unable to manage risk within an acceptable and appropriate level commensurate with the criticality of the application.

Sincerely,

John B. Sherman