



NAID-Europe

Avenue Jules Bordet 142

1140 Brussels, Belgium

Phone: 32-28080364 / Email: info@naideurope.eu

Standards Committee for Information Technology and Applications
German Institute for Standardization (DIN)
AM DIN-Platz
z.H. NA 043-01-51 AA
Burggrafenstraße 6
10787 Berlin
Germany

25 January 2012

Re: Comment on Draft Standard DIN 66399-2011-09

Dear Committee Members,

The National Association for Information Destruction, Inc., (NAID) is a non-profit trade association of secure data destruction services. While based in the United States, the association represents the secure data destruction industry around the world through regional chapters.

Our European chapter (NAID-Europe) currently represents over 100 member locations in the region, including many in Germany.

We commend the committee for its work on the proposed standard (DIN 66399-2011-09). The committee's efforts to create a clear methodology for secure destruction, emphasizing processes as well as particle size are completely consistent with NAID's philosophy.

As the committee is well aware, DIN standards are highly respected around the world. Therefore, NAID urges the committee to keep in mind their work on data destruction standards will resound globally.

In light of DIN's global influence, on behalf of our more than 1,800 secure destruction member companies in areas as diverse as China, South Africa, Malaysia, the United States and Canada as well as Germany and the rest of Europe, we ask the committee to consider modifying the proposed standard slightly.

The points for which we ask consideration are the following:

- 1) Hands-free processing of documents.

The draft standard requires hands-free processing for all Protection Class 3 documents and higher when entrusted to a third party for destruction. It is our position that this security measure does not increase security as desired.

The underlying premise of this specification assumes that destruction completed by the data controller or data originator is supervised. In reality, most such destruction is unsupervised in the business environment. On the other hand, destruction services provided by a third-party contractor with a contractual and fiduciary responsibility to destroy the materials are highly supervised. In addition, there are more checks and balances in place for a monitored secure destruction processing scenario than an office environment. Employees in destruction services are better screened, better trained than most employees and personally bound by employer contracts to perform fiduciary duties.

We believe focusing on a hands-free requirement creates a false sense of security. It may lead some to believe that in-house destruction is more secure. It simply is not so. It also may encourage the use of inferior destruction services which, even though they offer the hands-free service, lack other critical security policies and procedures, resulting in inadequate security overall.

Implementing a hands-free requirement diverts attention from the real issue and, as a result, could make the situation worse.

A more legitimate source of security would be to make sure the data destruction company has processes for screening and monitoring employees at all times, as well as a specific fiduciary contract with each employee.

- 2) Limited recognition of the security improvements inherent to the commercial grade processing scenario.

As with the existing specification, the committee has recognized the additional security provided by high-volume destruction of documents on a commercial basis. In the proposed standard this is reflected by graduating security levels from P1 to P2 and from P2 to P3 when a high-volume, commercial data destruction service comingles destroyed particles in a high-production environment.

We urge the committee to apply this same recognition to all security levels.

Commercial data destruction services destroy high volumes of material that are randomly comingled in the process. In addition, the process is performed by companies and people who have a legal contract to properly and securely execute their responsibility in a focused manner. Both of these factors lead to higher security than is available from in-house destruction processes.

Further, unlike the vast majority of in-house destruction processes, the commercial destruction process represents a closed loop and it limits access to the destroyed particles after the destruction process.

Over the last decade, a number of initiatives have demonstrated how easily even small paper particles can be reconstructed. A recent contest hosted by the U.S. Defense Advanced Research Projects Agency (DARPA) challenged participants to reconstruct finely shredded paper. Participants demonstrated just how easy it can be done using conventional technology.

Any system that controls the destroyed particles is demonstratively more secure than a process where the particles are not controlled. More specifically, the security of level P3 when it is destroyed by a commercial contractor who controls the particles afterward is significantly more secure than security level P4 particle size if those particles are casually discarded.

In consideration of this point, we urge the committee to consider allowing a single security level upgrade to commercial destruction services that directly recycle the comingled and baled particles.

As stated previously, DIN's influence on data destruction in Germany, Europe and around the world, are well earned. The fact that this committee is actively transforming the standard from a static particle size orientation to a process orientation is further evidence of its leadership in this area.

NAID is honored to be submitting comments to such an illustrious body and participating in such an important discussion.

I am happy to answer any questions or assist you any way.

Sincerely,

A handwritten signature in black ink, appearing to read 'R. Johnson', with a stylized flourish at the end.

Robert Johnson
Chief Executive Officer
National Association for Information Destruction, Inc.